APPLIED COURSE
Ph: +91 844-844-0102

COMPUTER - NETWORKS : Why?

Tasks uses computer Networks.

- browsers
- Email - client
- Skype / whatsapp - call
- Remote access

- Laptop
- desktop
- Smartphone
- Smartwatch

→ computational device can use computer networks.

SDE, Bigdata Engineer, Network Engineer
↳ may end up doing networking.

* WIFI / LAN / 4G → These are devices and technology used to communicate in networking

* Terms you will encounter while this course:

- MAC address
- IP - address
- Router
- WIFI
- DNS
- Subnet
- HTTP / HTTPS

* Wireshark is one of the software used for the analyzing the scenario of incoming and outgoing traffic.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

OSI - Model (Open System - Interconnect)

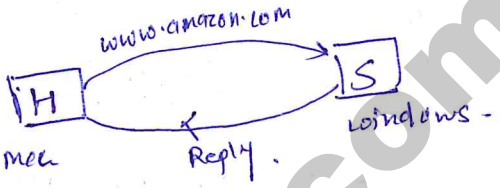
This model gives you the high level overview of how do you transmit data from one computer to another computer.

→ Reference - model.

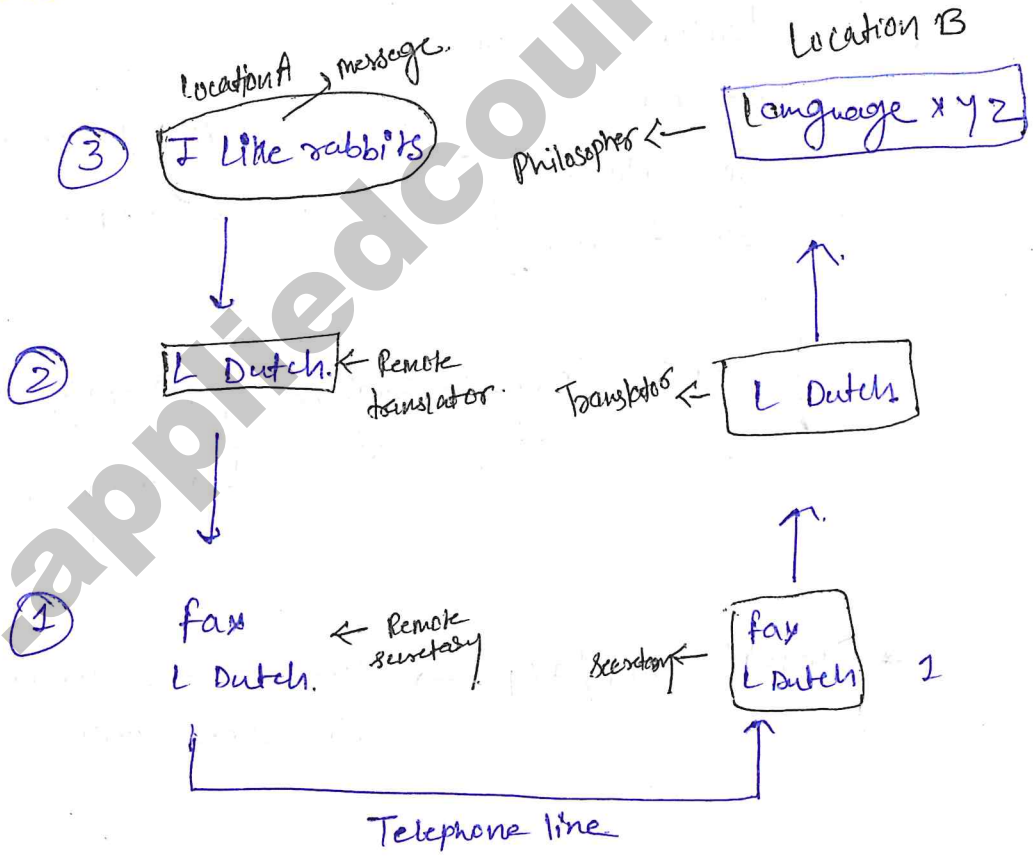
→ 1970's and 80's (1984)

→ Protocols (Rules) and Layered - system

→ host, address.



Layered approach →

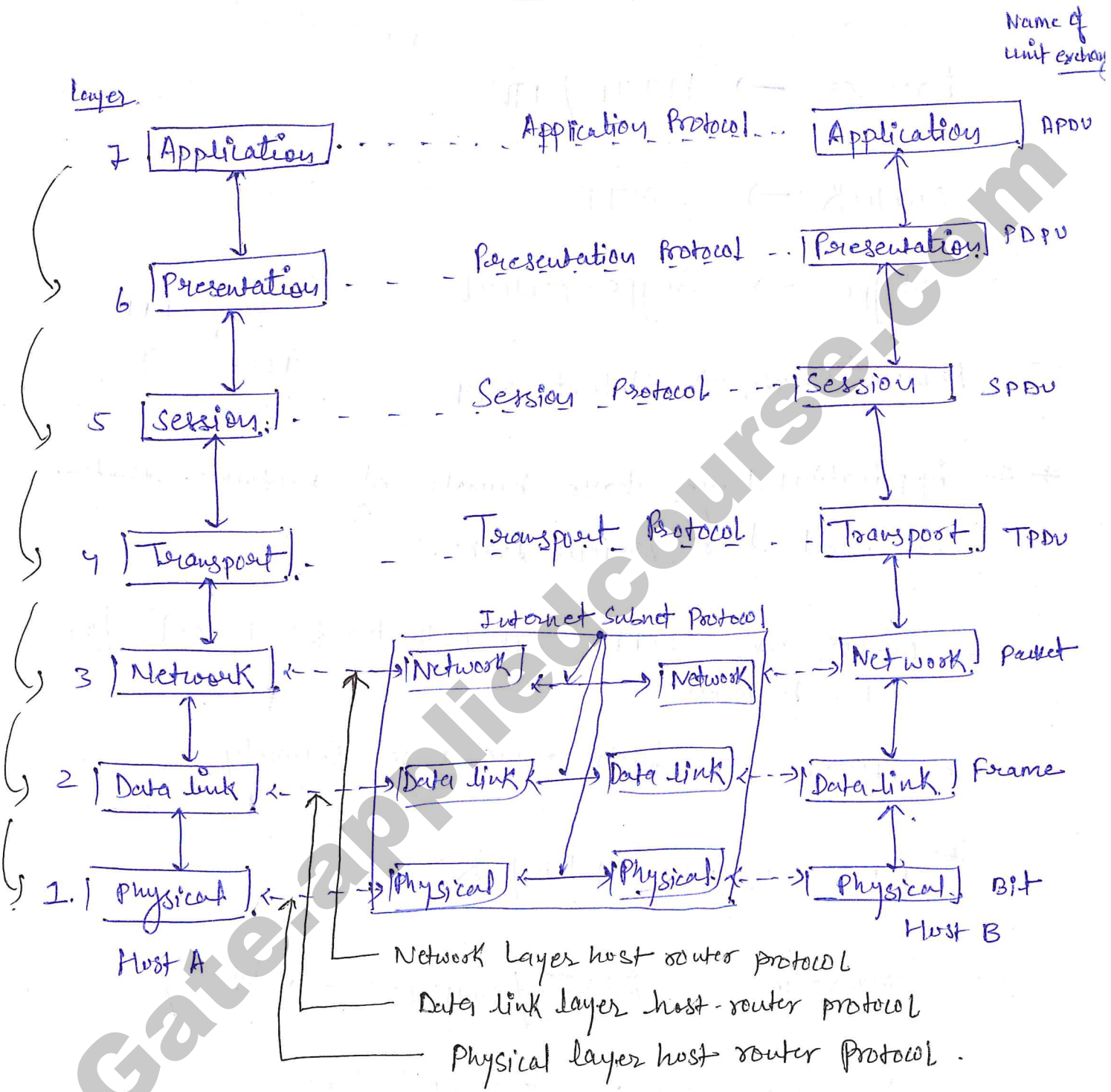


* CO/OS ⇒ address means Memory addresses.
* Computer networks ⇒ address means IP address / MAC address

Gateappliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

OSI Layers



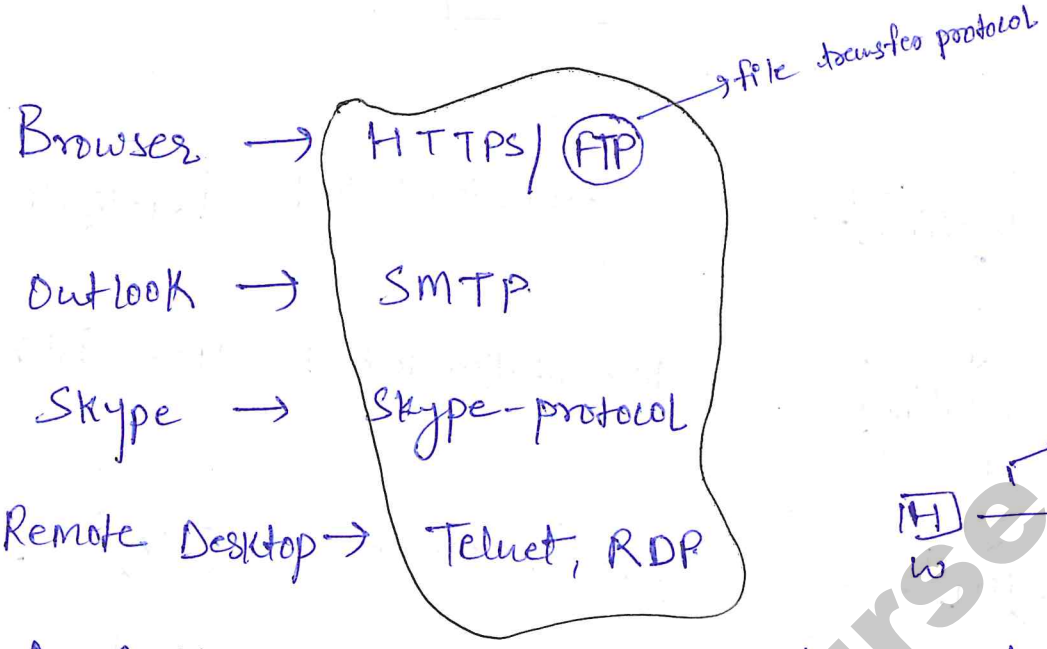
OSI REFERENCE MODEL

→ In coming course we are going to learn about each of these layers in detail.

Gateappliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Application Layer :—



** Application Layer have bunch of protocols that are used for various tasks.

* Outlook uses SMTP (simple mail transfer protocol) for transfer mail.

* HTTPS to fetch a web page securely.

* PRESENTATION LAYER :—

→ Translation — ASCII / UNICODE → binary

→ Data compression — Text / Audio / video

→ Encryption — Passwords

SSL (Secure Socket Layer)

DS and Algo (HuffmanAlgo)

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

→ Translate one form to another form.

→ Compress the data from one form to another form.

→ Encrypt the data from one form to another form.

Session Layer :—

→ Establish, manage and terminate connections.

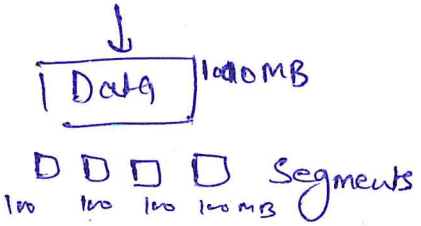
→ Authorization and Authentication.

* Example of session is login and logout.
* Authentication using userid and password.

Most modern browsers manages these tasks → { Application, presentation, Session Layer }

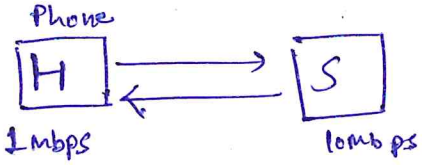
Transport Layer :—

→ Segmentation



* Data is breaking into segments to transfer one chunk of data

→ FLOW - control

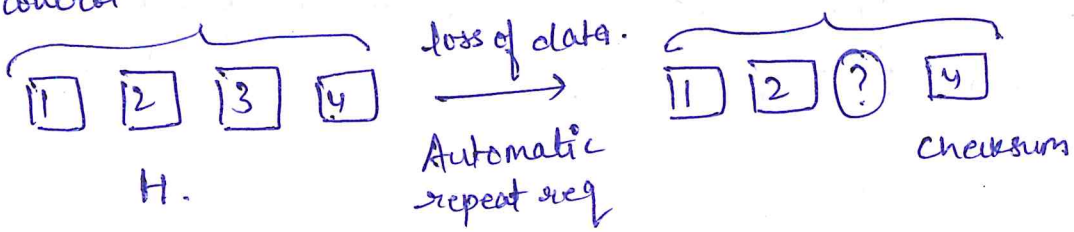


* At what speed the host wants the flow from the server.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

→ Error control



There can be lot of errors while transmitting the data. Error control mechanism helps us to detect and correct the errors. We use checksum, CRC etc.

*

* Port no. 80 used widely for browsers.

→ TCP VS UDP.

Slow	fast, lossy
lossless	no feedback
feedback	videochat
webpage, email	
Connection oriented	Connection less.

Gate.appliedcourse.com

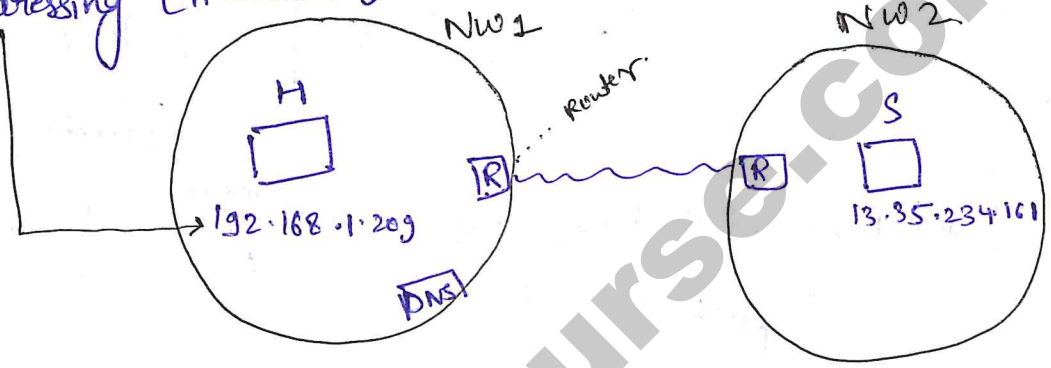
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Network Layer:-

→ Packets [Segment + Source and destination address] ⇒ We include Ip addresses in the TCP packet.

→ Logical addressing (IP address)



* Range of ip address: 0.0.0.0 to 255.255.255.255
* You can use wireshark to capture the packets and also you can know various types of packets and lot of details about them.
* The task of routing is to route the packet from source to destination.

→ Routing Mask.

* The mask number help to get the network address by performing AND operation.

* DNS (Domain name system) is used to connect host name like amazon.com to the ip address.

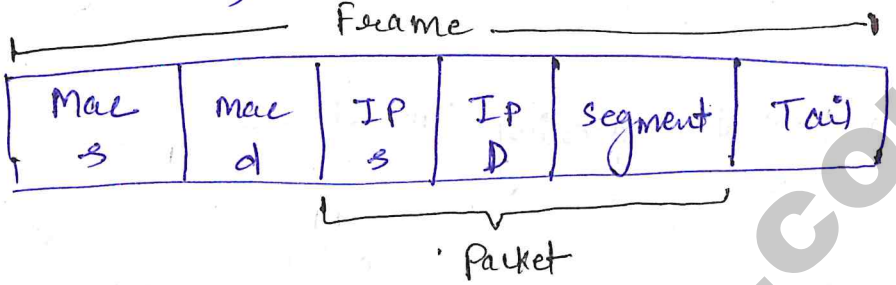
→ Path determination: To find most appropiate paths. [Graph theory application]

Gate.appliedcourse.com
gatecse@appliedcourse.com

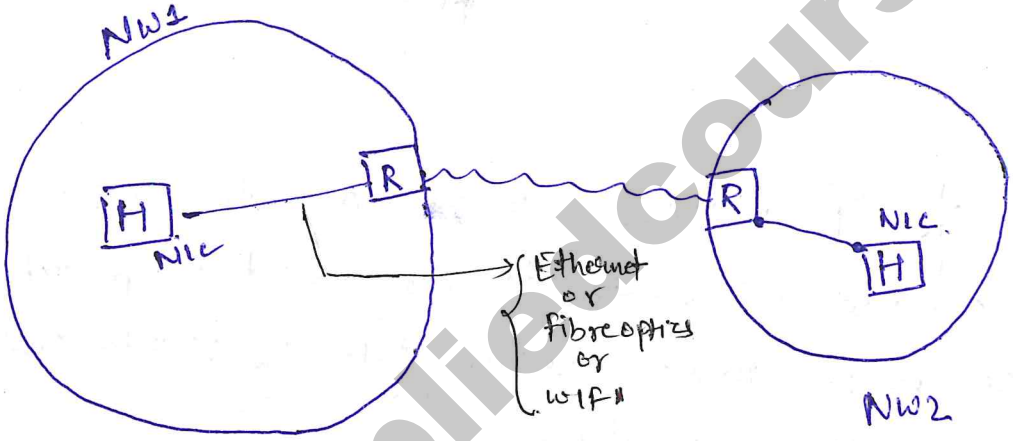
APPLIED COURSE
Ph: +91 844-844-0102

Data Link layer :- (L3)

→ Physical-addr (MAC)



* Data link layer we called data. of a frame

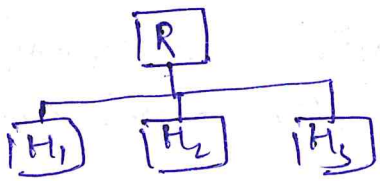


* Every host has a unique mac address.

* Data link layer added mac addresses.

→ Access to media (copper wire, fibre-optical-wire, wireless)
Ethernet

→ (MAC) Media-access-control : collision free



* All of the host can not send packet at same time. MAC ensures avoid collission

Gate.appliedcourse.com
gatecse@appliedcourse.com

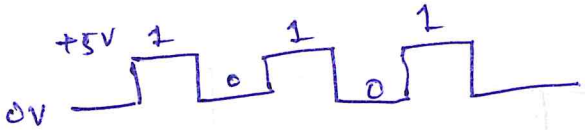
APPLIED COURSE
Ph: +91 844-844-0102

→ Error detection : Tail

It is added in the tail part like checksum.

Physical layer :—

→ Bits to signals



Copper wire

Laser - ON | off
fiber-optics

radio signals
wireless

Physical layer job is to transmit from bits to signal based on the medium you used.

1984
Reference model [Theoretical]

OSI

Application → DNS, HTTP | S
Presentation
Session

Grouped together

Application → Data.

TCP | IP (practical)

Transport → Transport (TCP/IP) → Segments
Network. → Network. → Packets
Data link.
Physical → Physical → Frames | Bitsream. (stream of bits.)

* TCP/IP widely used practical model while OSI is Ref model.
* ~~Segments~~ are also called datagrams.

gatecse@appliedcourse.com
Gate.appliedcourse.com

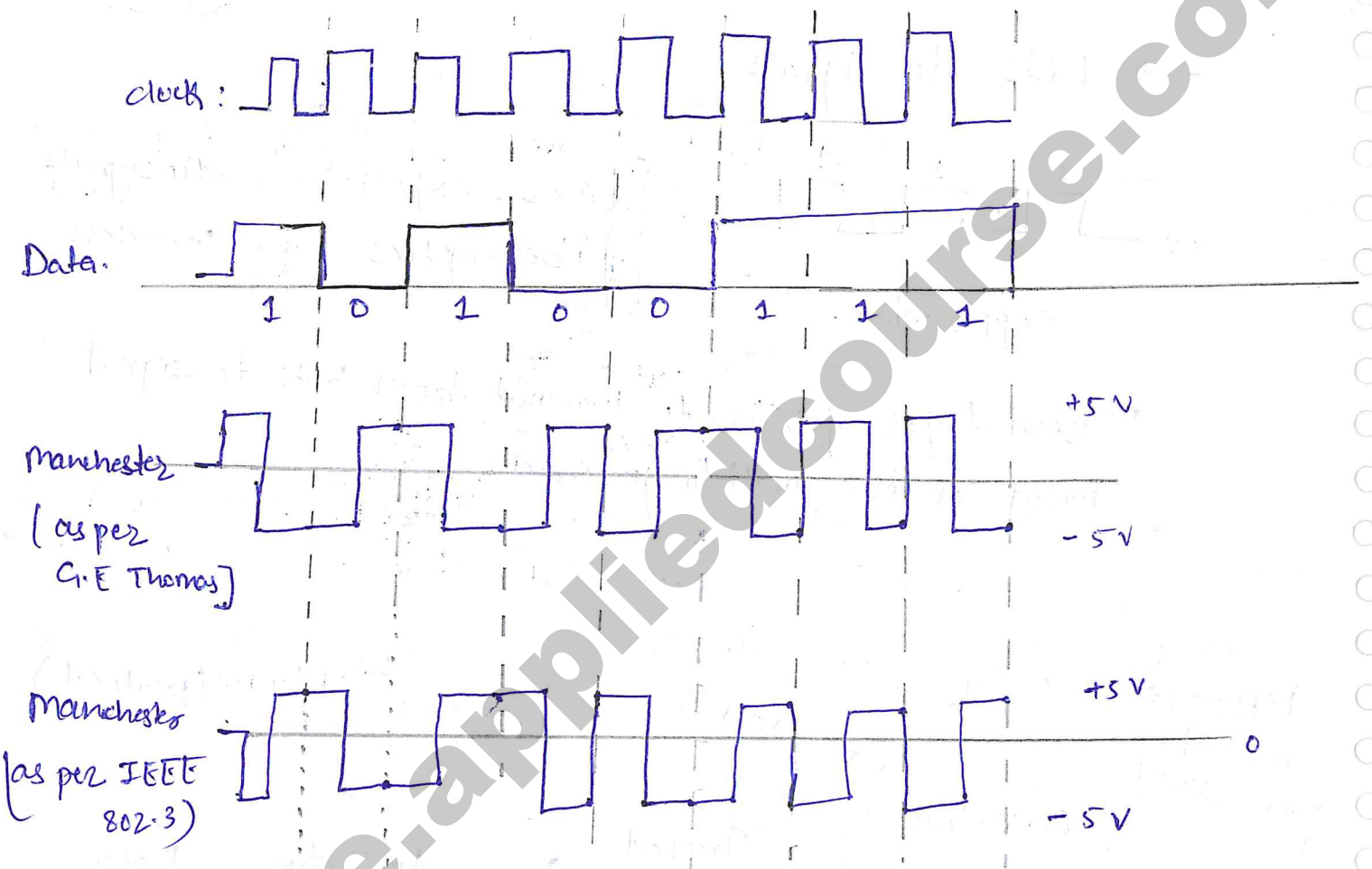
APPLIED COURSE

Ph: +91 844-844-0102

Physical Layer: —

Bits to signals.

Encoding: — * You have each clock cycle.



GE Thomsay follows +A, -A → 1 ; A, -A → 0

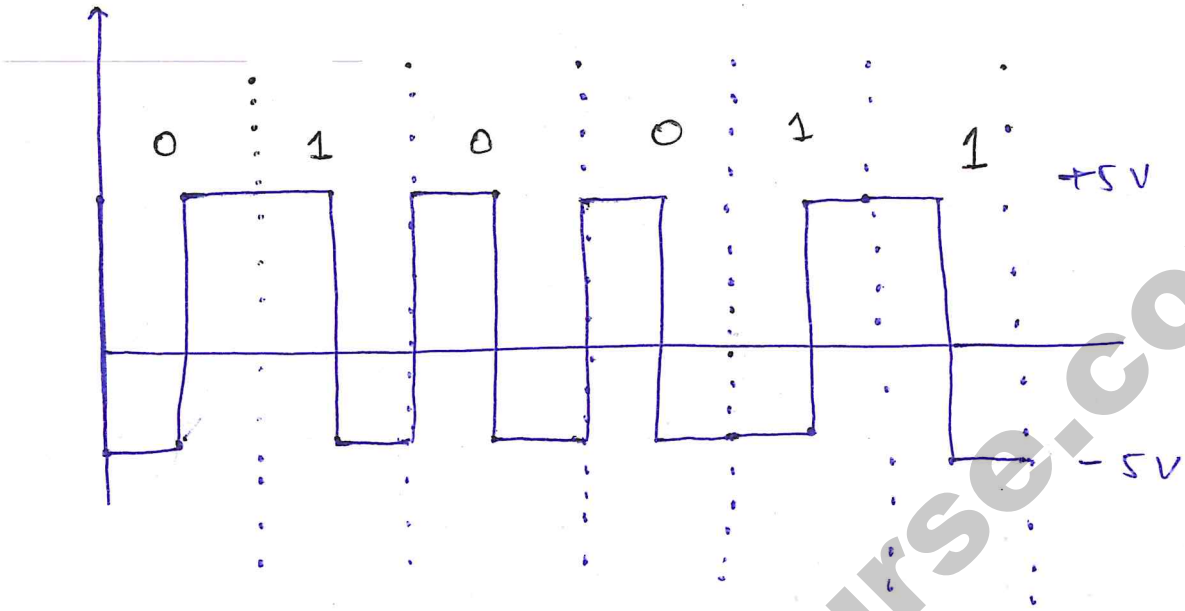
IEEE 802.3 → +A, -A → 1 ; +A, -A → 0

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Differential manchester encoding



In differential manchester encoding, the transition at the middle of the bit is used only for synchronisation.

The bit representation is defined by the inversion.

Bit 0 → Inversion

Bit 1 → No inversion.

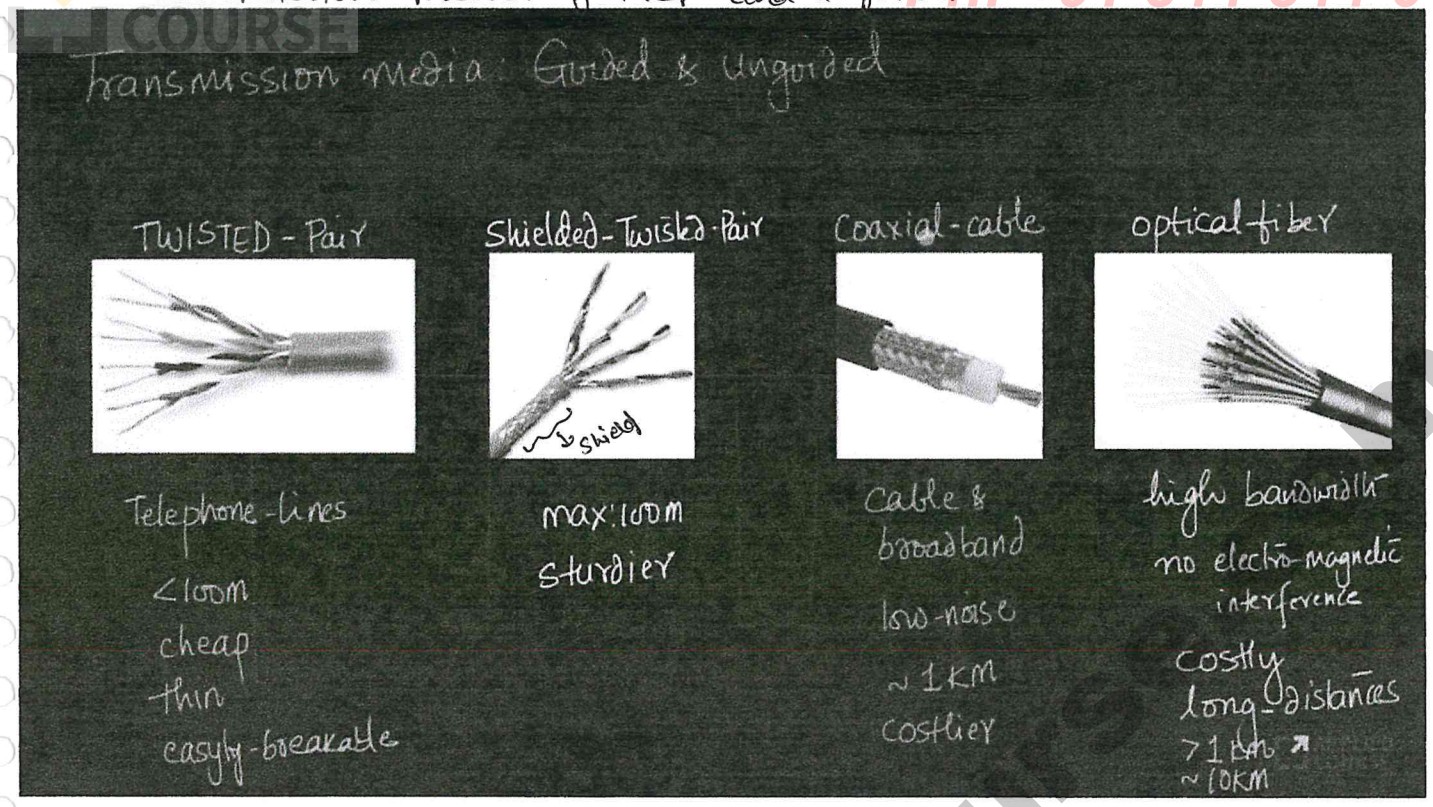
Whenever 0 arrives we invert the transition whenever 1 arrives we don't invert and continue the transition.

* In diff manchester encoding transition is from -v to +v or +v to -v. We are using + and - because manchester / diff manchester are bipolar encoding.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE Ph:-+91 844-844-0102

Transmission media guided and unguided :-



All twisted pair, Shielded-Twisted pair, co-axial cable and optical fiber are guided media.

Twisted pair → Simplest media, invented by Alexander grahmbell Modem connect to telephone lines and also to computer for internet. Here pair of copper wire twisted amongst themselves.

Shileded Twisted pair → They are shielded with aluminium shield. It makes it strengthful and also less interference.

Co-axial cable → Cable connection (DTH) used this most. It is costlier and work 1 KM distance. we can use the repeater to strength the cable.

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Optical fiber → The laser beam is pass through it.
It uses the concept of total Internal reflection (TIR). It can work upto 10KM

UNGuided media: —

Infrared
↓
* TV remotes uses this technology.
* Short range can't penetrate wall.
* Early 2010-2012 Smartphones also used it.

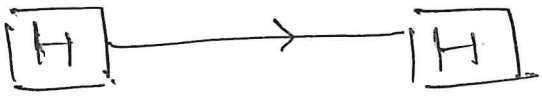
wireless
↓
* radio-waves (WiFi, 4G)
(weather-condition)
↳ 15 KM.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

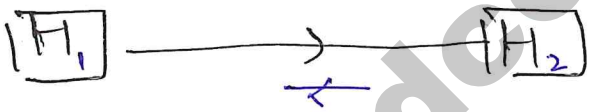
Transmission modes: -

Simplex →



In Simplex we can send the data only one direction.

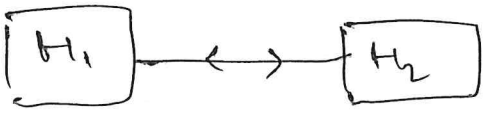
Half duplex →



In duplex we can send the data in both the directions but not at the same time.

Either host 1 to host 2.
or host 2 to host 1.

Full duplex →



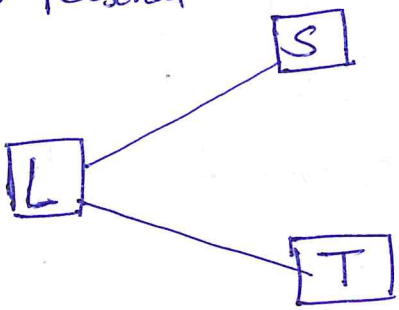
In full duplex we can send the data in both the directions. we can also send the data in both the directions at the same time.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Network Types :-

① PAN → Personal area network.

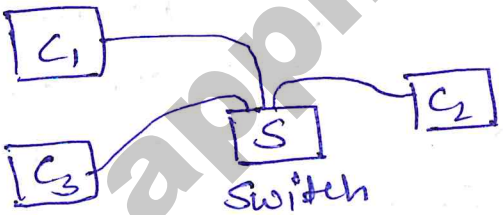


USB - cable
Bluetooth → most popular
NFC → Payment systems.
Infrared ← IR

NFC → Nearfield communication

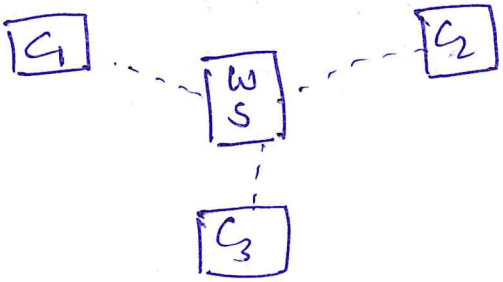
* A network that you can construct using the personal devices without use of infrastructure.

② LAN [Ethernet-LAN]



Local area network. uses networking devices like hub, switch, bridges etc.

③ WLAN (WIFI)

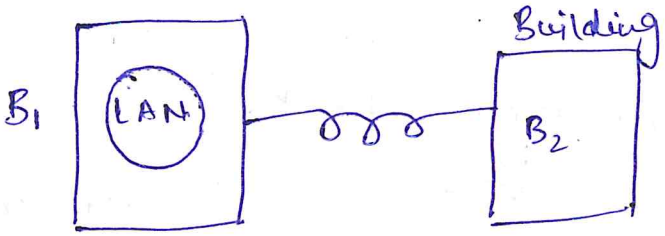


* The repeater gives the boost to the signal and transmits it further.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

④ CAN. (Campus Area Network).

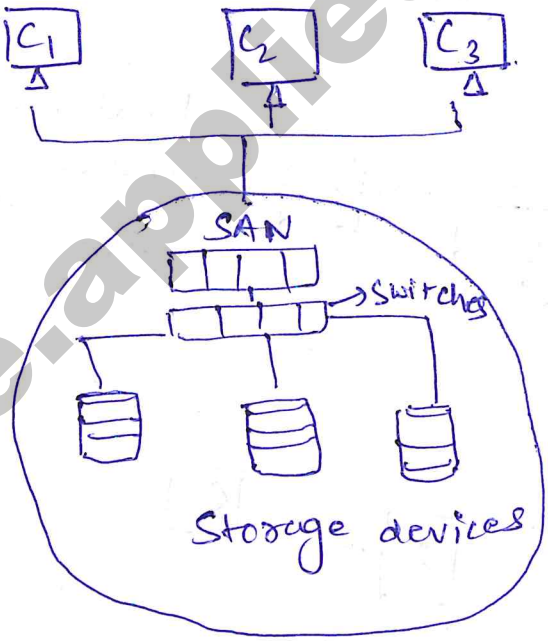


Connection at the campus level is called CAN.

⑤ MAN → Level of Town.

⑥ WAN → country, Europe, world
eg: Internet

⑦ SAN [Storage area network] :-

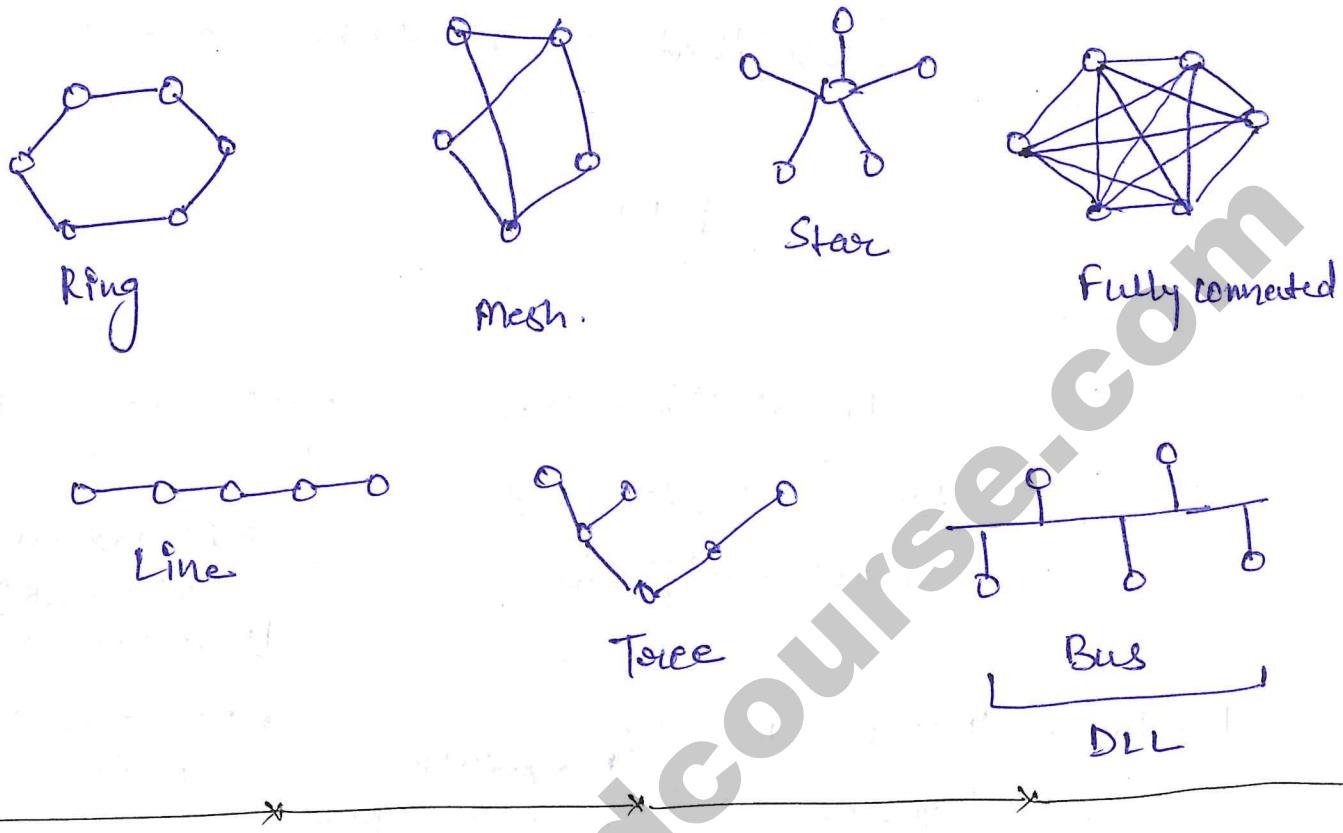


All the systems are connected to very fast switches and router. The transfer of data from these storage devices.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Network Topologies:

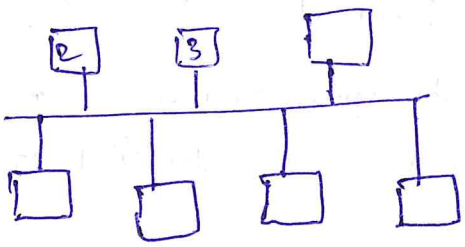


1

DATA LINK LAYER

(1) Access to media (fiber optic, wifi, twisted cable)

(2) Media-access-control



* It is going to control which pair of media will transfer the data.

(3) Error-detection → If any collision then we have to detect the collision.

* Frame is the unit for data link layer.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

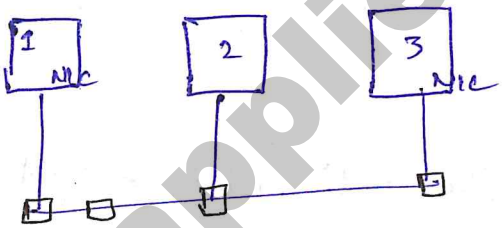
(4) Flow control → Ensures that two hosts will control at what rate data should be transfer so that there will be no. errors.

DLL

Logical link sublayer
flow control, ACK and error notification

Media-access-control sublayer
MAC address (wireshark)
[12 digit alpha numeric]
↳ who access the media

Hardware: NIC ; WIFI-card ; .... → Available in your system.
Layer-2-Switch



1 → 3

* MAC address: → 48 bit address. [Unique]
* In wireshark you can see a UDP packet where that packet will be showing mac address.

* Switches, layer 2 switch used for connecting hosts.

H — S — H
↳ Amplify the signals also.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Delays :-

① Transmission delay (T_t)

How much time it will take to place the data on the physical wire :-

B = Bandwidth in bps L : # bits in a packet

$$T_t = \frac{L}{B} \text{ sec}$$

B bits → 1 sec.
1 bit → $1/B$ sec.
L → L/B sec

② Propagation delay :- (T_p)

D : length of wire
V : velocity

Propagation time is how much time it will take to send the data from one point to another point.

$$T_p = \frac{D}{V} \text{ sec}$$

* Eg D = $2 \cdot 10^3$ KM
V = 70% of speed in vacuum $V = 3 \times 10^8$ sec.

$$T_p = \frac{2100}{2 \cdot 1 \times 10^8} \cdot \text{sec} = 10^{-5} \text{ sec} = 10 \mu\text{sec}$$

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Note:→

1 ms = 10^{-3} sec
1 μs = 10^{-6} sec
1 ns = 10^{-9} sec

Data:
1K = 2^{10} = 1024

Bandwidth:
1K = 10^3

↓
Typical convention

Eg. L = 1000 bits
B = 1 Kbps

T_t = $\frac{1000 \text{ bits}}{1 \text{ Kbps}}$ = $\frac{1000}{1000}$ = 1 sec

Eg L = 1 Kb
B = 1 Kbps

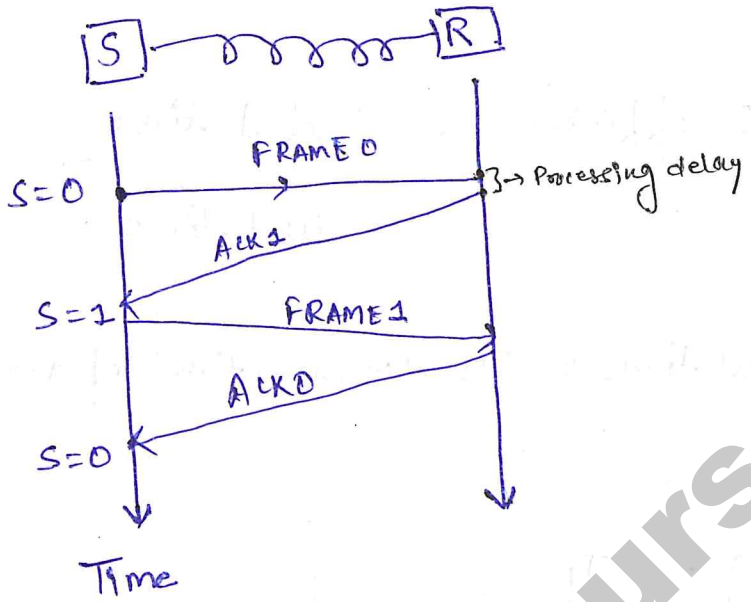
T_t = $\frac{1024}{1000}$ = 1.024 sec.

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Flow control: STOP and WAIT (ARQ): → Automatic repeat request



The flow is like 0, 1 0 1 0 1 . . .

→ Here in stop and wait, the sender send the frame zero and receiver send the Ack 1.

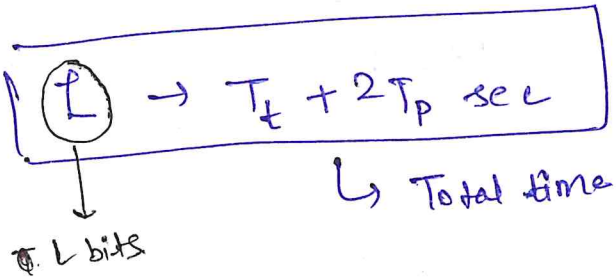
→ The sender waits until the Ack received from the receiver.

Calculation of total time for sending 1 packet/frame.

1 frame = $T_t + T_p + T_{pr} + T_t^a + T_p$

T_t^a → v.v small

T_{pr} → processing time is negligible



Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Calculation of "Efficiency".-

η = efficiency = $\frac{\text{Useful time}}{\text{Total time}}$.

↳ Useful time = Transmission time of frame.

* $\boxed{\eta = \frac{T_t}{(T_t + 2T_p)}}$ ——— (1)

* Let's divide the eq 1 with T_t in both numerator and denominator.

$$\eta = \frac{1}{1 + 2(T_p/T_t)}$$, $\boxed{a = \frac{T_p}{T_t}}$

* $\boxed{\eta = \frac{1}{1+2a}}$

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Throughput / Bandwidth - utilization / Effective Bandwidth.

* Throughput is measured on bits per seconds.

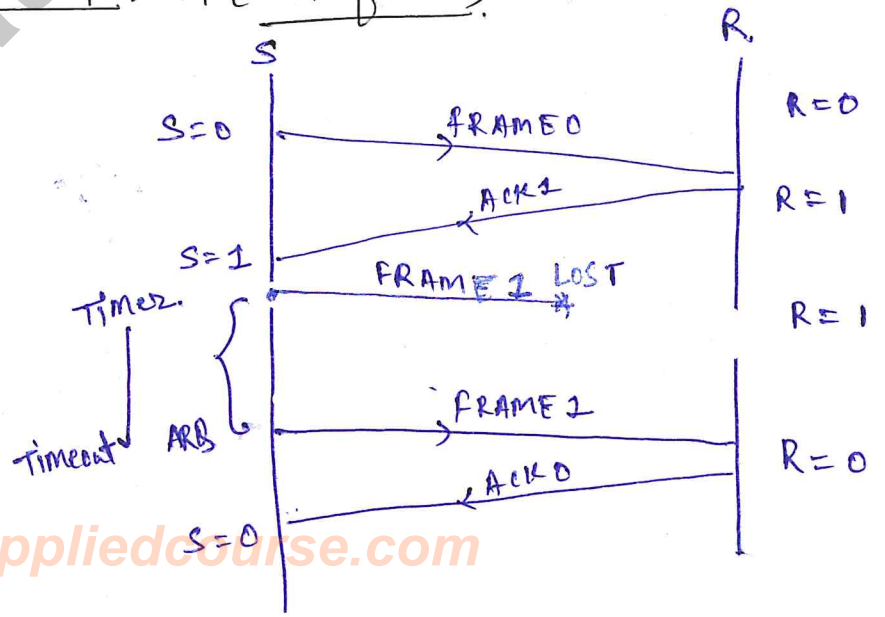
* **Throughput = $\frac{L}{T_t + 2T_p}$** $\Rightarrow \frac{\text{Datasize}}{\text{Total time}}$

$= \frac{\frac{L}{B} \times B}{T_t + 2T_p} = \frac{T_t \times B}{(T_t + 2T_p)} = \eta \times B$

* **Throughput = $\eta \times B$**

* In total time how many bits you send is called throughput.

STOP and wait (lost frame)

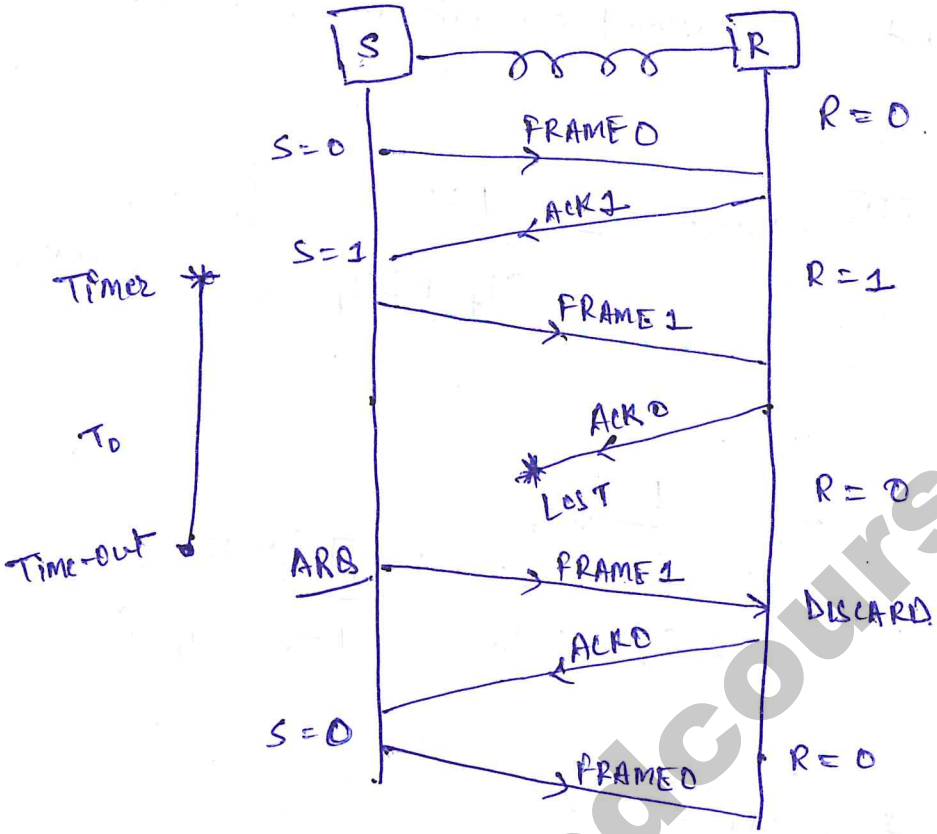


* Here when the frame get lost after some time when timer expires. It sends the same again.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

STOP & wait ARQ (Lost ACK- frame)

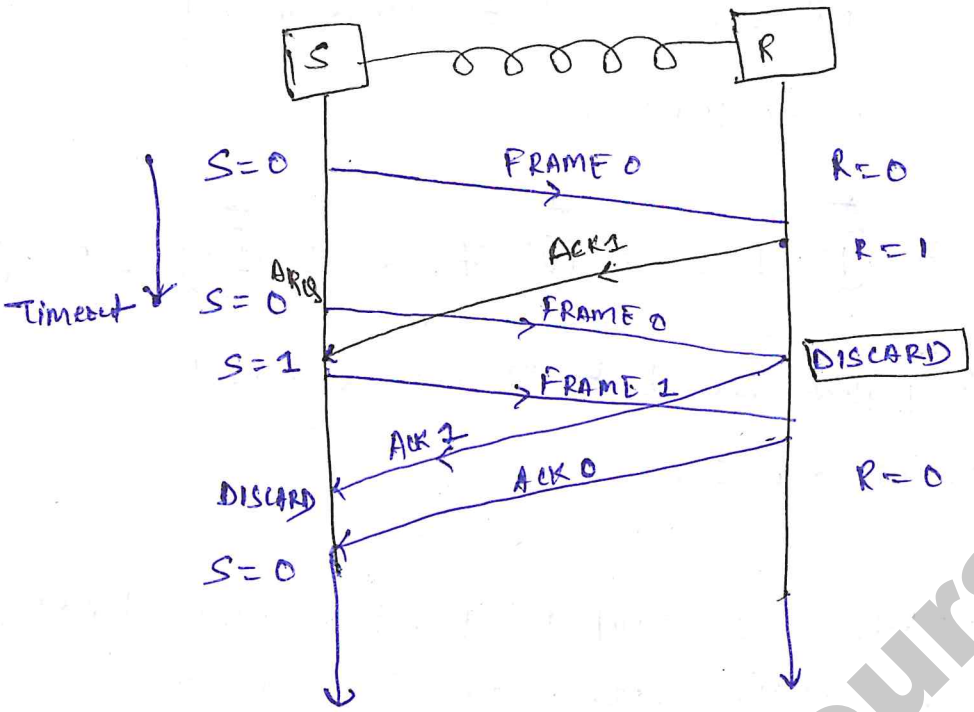


* Here when the Ack get lost. So after timeout Sender will re-send that frame. At the receiving end receiver find out it's a duplicate frame and simply discard that frame. Receiver now send the Ack again.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

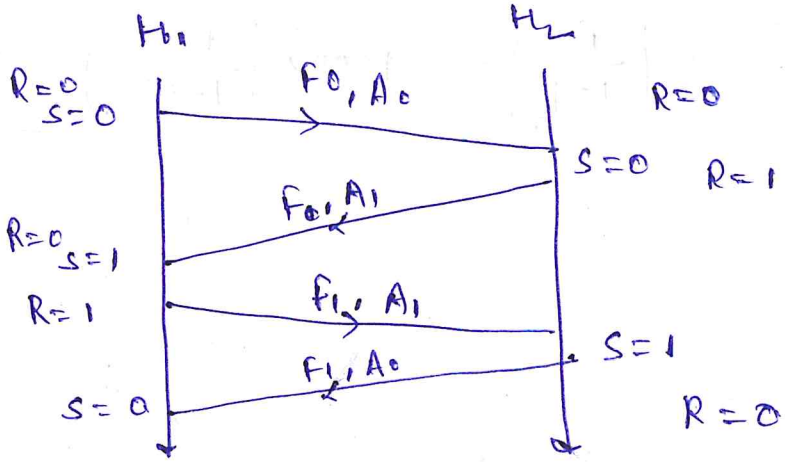
STOP and WAIT (delayed ACK)



In stop and wait when Ack gets delayed before that timeout occurs on the sender side and sender re-send the frame again. After sending the frame the sender's receive and Ack of the old frame and after some time again gets the ACK of the FRAME 0.

Sender's discard the Ack 1 because it is a duplicate ACK.

STOP and wait (Piggybacking) :-



* Piggybacking means with data we also send the Ack together to save the time.

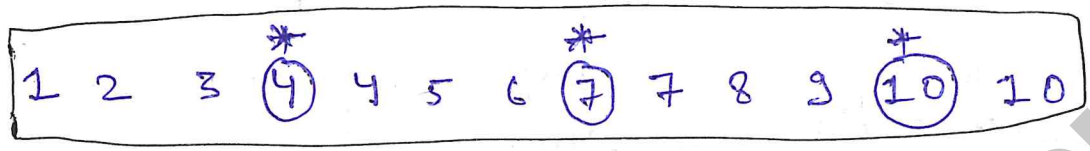
*. Here we are sending data to both the directions.

* Both hosts are sending data and receiving Ack synchronously

gatecse@appliedcourse.com
Gate.appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que In Stop and wait ARQ, a sender sends 10 packets of which every 4th packet is lost. How many transmissions are needed?

Soln → 

Every 4th packet is lost it means total Transmissions are 13.

Que: If 1000 packets are send using stop and wait ARQ. The error probability is 80%. No. of transmissions needed?

Soln: 80% probability = $\frac{1000 \times 80}{100}$ = 800 packets

= $\frac{800 \times 80}{100}$ = 640 ....

So, $n + np + np^2 + \ldots \rightarrow$ G.P.

$\Rightarrow n[1 + p + p^2 + p^3 \ldots]$

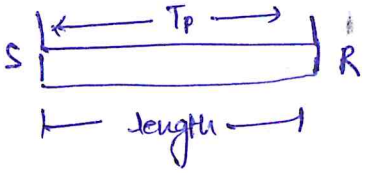
$\Rightarrow n\left(\frac{1}{1-p}\right) = 1000 \times \left(\frac{1}{1-0.8}\right) = \frac{1000}{0.2}$ = 5000 packets.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Capacity of a channel / medium: Maximum no. of bits on the wire.

$$= BW \times T_p \text{ bits}$$



Cap ↑ ⇒ BW ↑

Cap ↑ ⇒ T_p ↑ ⇒ length ↑

Que:

BW = 2·1 Mbps

T_p = 1 sec.

frame size = 10^3 bits

Capacity = ? Capacity (full duplex) = ?

Soln. Capacity = $2 \cdot 1 \times 10^6$ × 1 sec = $2 \cdot 1 \times 10^6$ b = 2100 frames.

Capacity full duplex = 2100 + 2100 = 4200 frames.

In Stop and wait ARQ

$$\text{Efficiency } (\eta) = \frac{1}{4200}.$$

In Stop and wait protocol we are sending only one packet in round trip time. RTT means = $2T_p$.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

* η = No. of packets at any time on the medium / Capacity

Que. T_p = 1 ms T_t = 1 ms

No. of packets can be transmitted before waiting for an Ack of the 1st packet.

Soln. S ——oooooo—— R

It means capacity.

1 packet → T_t sec

$\frac{1}{T_t}$ packets ← 1 sec

Total time = $T_t + 2t_p$

In total time we can place = $\frac{T_t + 2t_p}{t_t}$ packets

$\left[t_p / t_t = a\right]$ = $1 + 2a$ [max packets we can place]

= 3 packets (Ans)

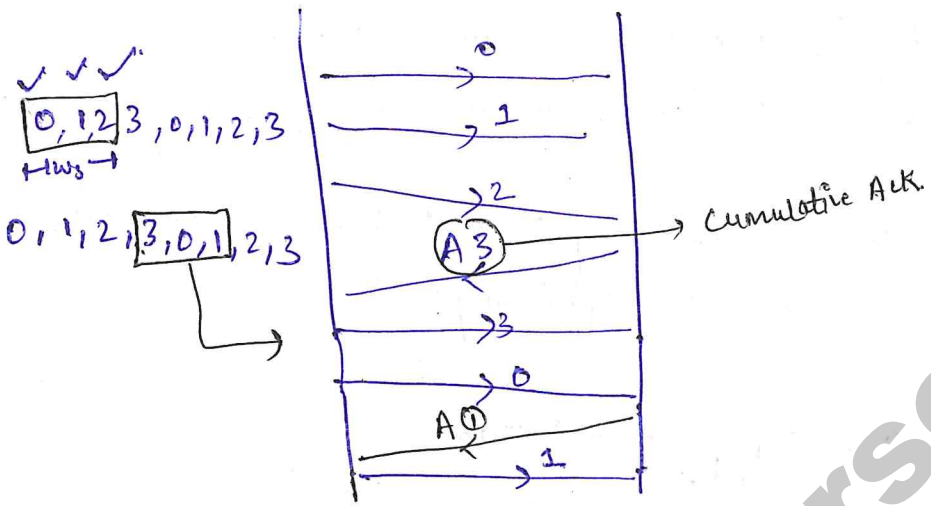
Capacity = $1 + 2a$.

η = Stop and wait = $\frac{1}{1+2a}$

Gate.appliedcourse.com
gatecse@appliedcourse.com

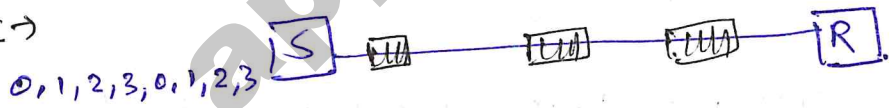
APPLIED COURSE
Ph: +91 844-844-0102

Sliding window protocols :-



* Here we are using 2 or more than 2 bits for sequence number.
* Using 2 bits we can represent 4 numbers. = 0, 1, 2, 3
* The window size is decide on the basis of sequence bits.

Concept →



In m bits = 2^m sequence no. possible.

$ws \leq 2^m$ [because we can not repeat same seq no. again]

and

$(ws \leq 1+2a)$

$$\text{Max}^m\ ws \leq \min(2^m, 1+2a)$$

capacity = 1+2a packets.

* For 1+2a packets → $\log_2(1+2a)$ bits are required.
* min m = $\log_2(1+2a)$, max m = ∞

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que : $T_p = 49.5$ ms

$T_t = 1$ ms.

(A) what is the max-window size.

(B) No. of bits for sequence no.

(C) If we have only 5 bit for sequence no. what is the efficiency.

Soln (A) $a = T_p / t_t = 49.5$ ms

$ws \leq \min(2^M, 1+2a)$

$1 + 2 \times 49.5 = 100$

$ws \leq 100$

(B) $ws = 100$ So, No. of seq no $= \lceil \log_2 100 \rceil$

$= 7$ bits

(C) using 5 bits we can send only

$0, 1, 2, \cdots 31 = 32$ packets

$\eta = \frac{32}{100} = 32\%$

* So, Efficiency of Slidingwindow

$$\eta_{Sw} = \frac{W_s}{1+2a}.$$

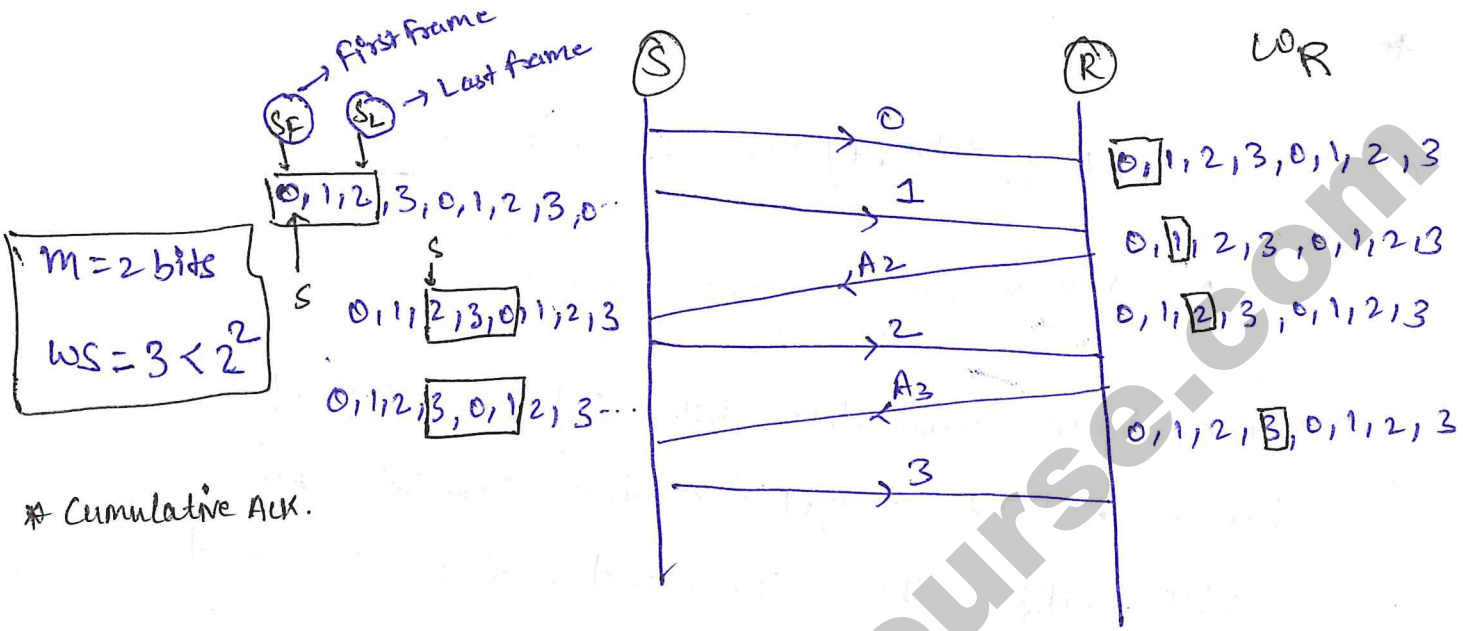
Throughput $= \eta_{Sw} \times B$

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Go-back-N ARQ

Sliding window

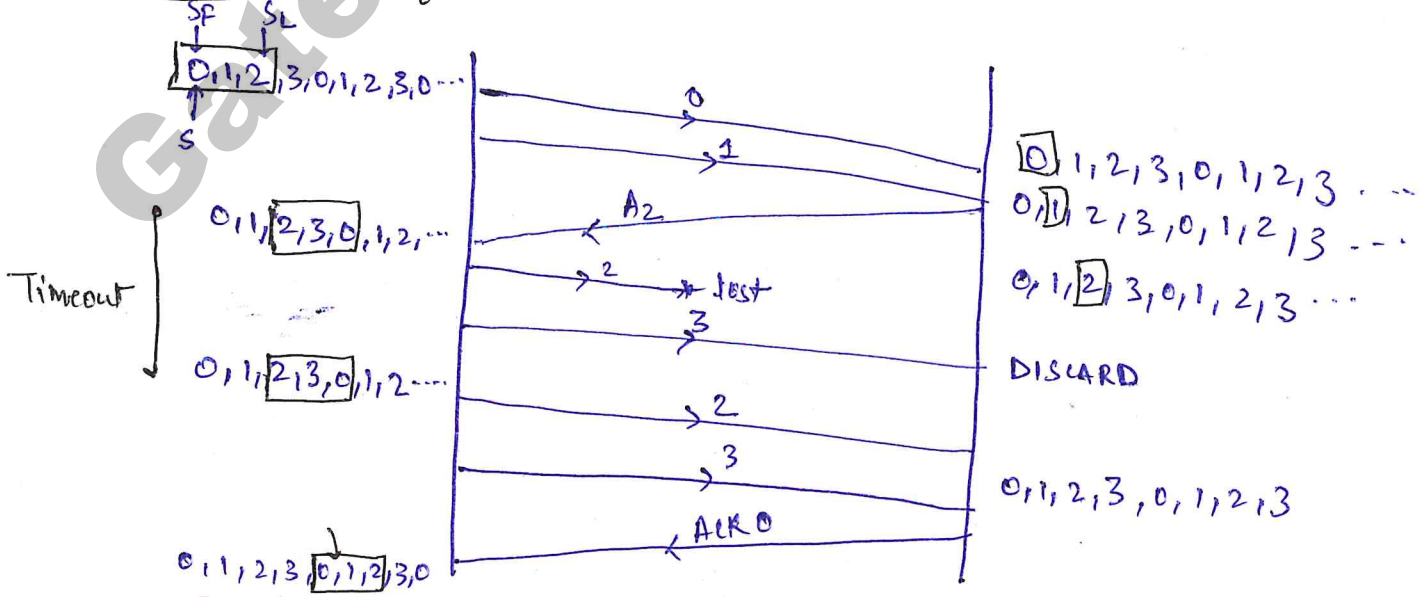


In Go Back N ARQ

$Sws \leq 2^m - 1$ m = seq no.

$Rws = 1$

GBN (Lost frame):



Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

* If the frame is lost, we are going back N and send all the frames in the windows again.

*

Case-1 GBN (delayed / lost / damaged ACK)

↳ ACK arrives before Timeout.

* We have cumulative ACK. If any ACK of frame will get delayed then the cumulative ACK will nullify it's. We need not to re-send the frame again.

* ACK arrives after Timeout

⇓

resend all frames.

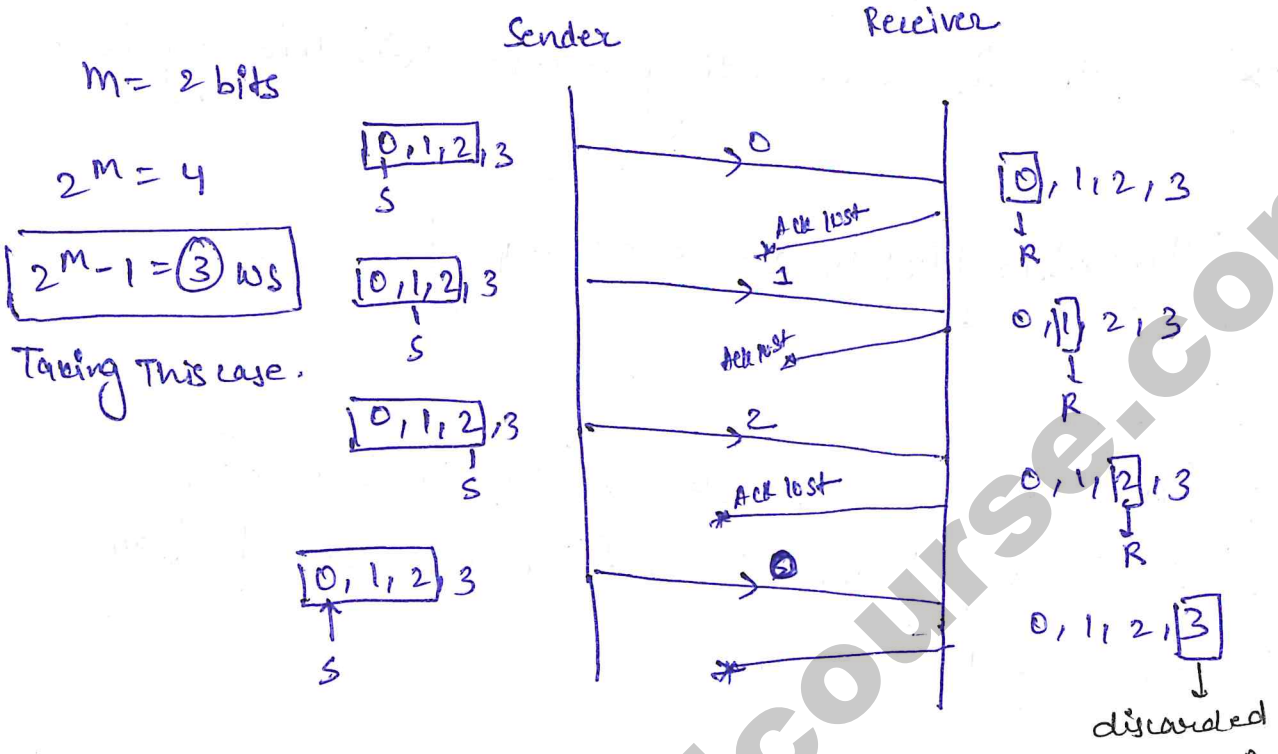
NOTE: [Receiver doesn't resend ACK in GO back N]

Gate.appliedcourse.com

gatecse@appliedcourse.com

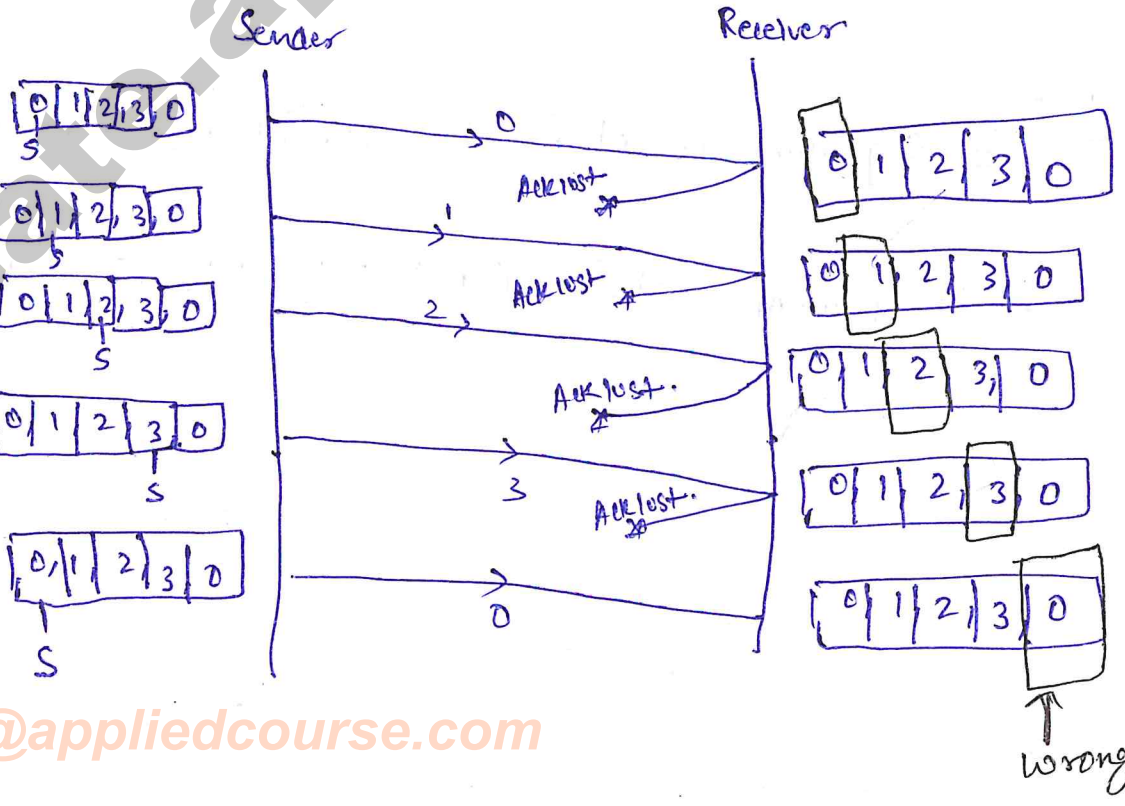
APPLIED COURSE
Ph: +91 844-844-0102

GBN : Sender-Size window $= 2^m$ vs $2^m - 1$



Here receiver are waiting for 3 and sender is sending zero which is correctly discarded when we take $WS \leq 2^m - 1$

Another case : $WS \leq 2^m$, Now check.



gatecse@appliedcourse.com
Gate.appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Here when we take $WS = 2^m$ then we are wrongly accepting 0, which should be discarded as sender is re-sending same window again.

Therefor | GBN $WS \leq 2^m - 1$

Que: GBN with WS = 3, Sender sends 10 frames. Every 5th frame is lost. max number of frames transmitted?

Soln →

1, 2, 3, 4, [5, 6, 7], 5, 6, 7, 8, 9, 7, 8, 9, 10, 9, 10

= 18 frames we send.

Concept →

Seq num needed in stop and wait = 2 = $W_S + W_R$ = 1 bit required

Seq num need in GBN = $W_S + 1$ = $W_S + W_R$

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

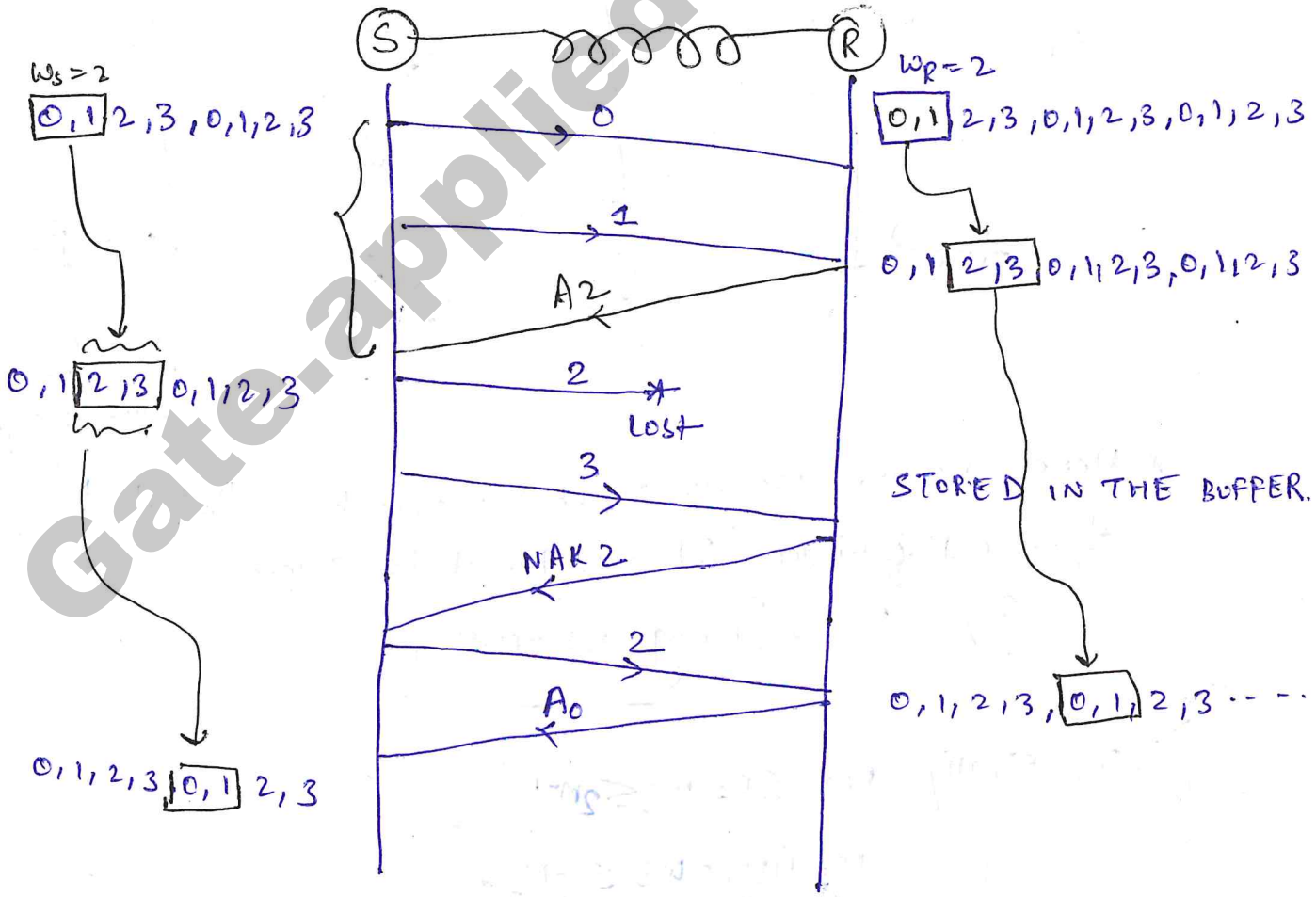
Selective Repeat SR (Sliding window)

→ Sender $w_S > 1$

→ Receiver $w_R = w_S > 1$

→ Re-send / Re transmission

- Implicit: R sends Ack for each good packet received. (Not accumulative)
- Explicit: R sends NAK for each corrupted / missing packet.
- * It supports both cumulative as well as individual Acks.

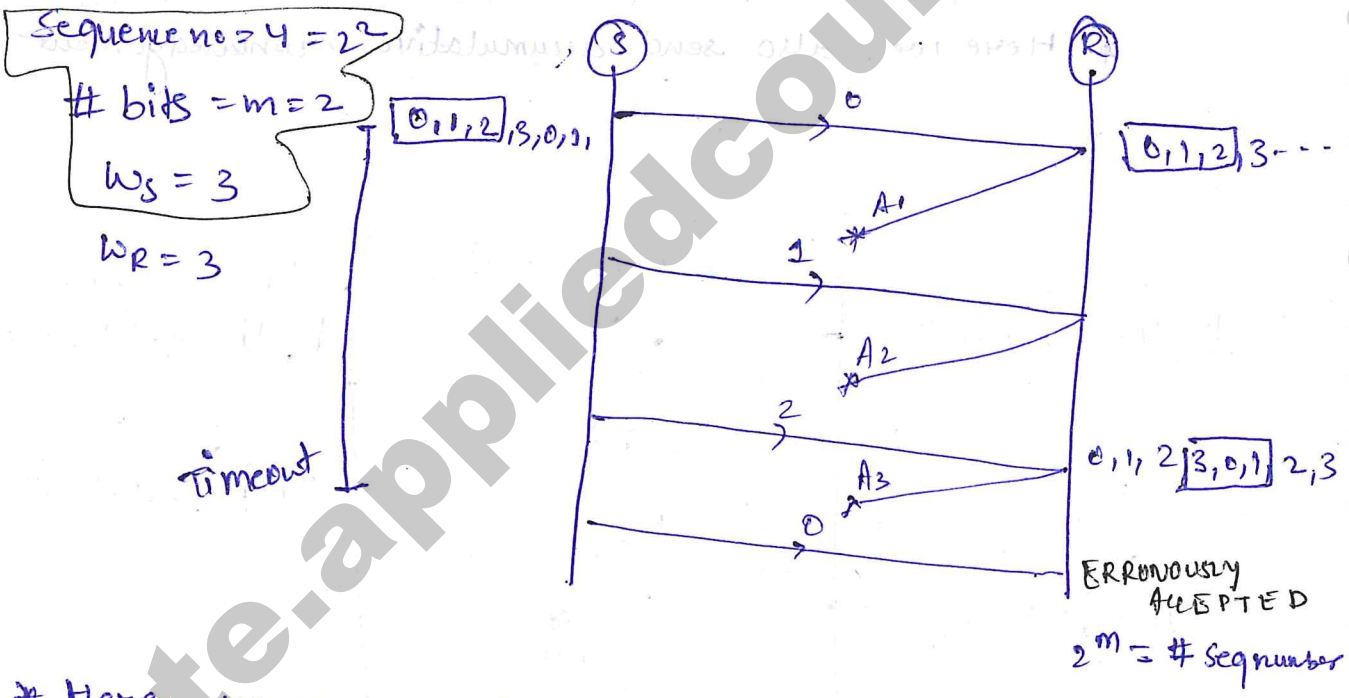


Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

* Here we are sending a frame size of two. When any frame of the window is lost. We send the NAK frame regarding it. We need not to send the whole window again. We have to send only the frame which is lost.

Check for window size



2^m = # Seq number

* Here we are wrongly accept zero as part of second window. It should not be accepted

$w_S \le 2^{m-1} = \frac{2^m}{2}$

So, $w_S = 3$ [wrong assumption]

*

So, Finally for $SR = w_S \le 2^{m-1}$

For $GBN = w_S \le 2^m - 1$

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Concept →

	S&W	GBN	SR
η →	$1/(1+2a)$	$N/(1+2a)$	$N/(1+2a)$
No. of buffers →	2_S 2_R	$N+1$	$2N$
min no. of seq no. →	2 [0,1]	$N+1$	$2N$
Retransmissions →	1	N	(1) NAK
Implementation →	Simplest	Moderate	Complex.
BW →	low	high	Moderate.

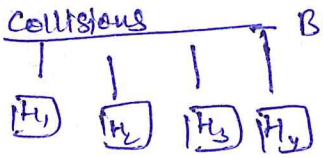
* Selective repeat is used in wireless situations.
* GBN can be ideal you can use fibre optic.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Multiple / media - Access Protocols :-

- Channelization Protocols
  - FDMA
  - TDMA
  - CDMA
- Controlled-access protocols
  - Reservation
  - Polling
  - Token Passing
- Random access protocols
  - Aloha
  - Slotted Aloha
  - CSMA/CD



→ Problem here is multiple host on the same channel, so there is chances of collision.

Channelization : Frequency division Multiple Access / Multiplexing

Freq: 100 MHz — 1000 MHz

100 - 199 MHz → H_1

200 - 299 MHz → H_2

300 - 399 MHz → H_3

⋮

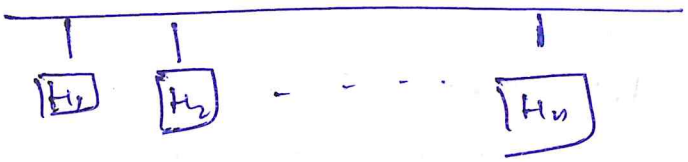
900 - 999 MHz → H_9

Here we are dividing the frequency such that no frequency will infere with each other

Gate.appliedcourse.com
gatecse@appliedcourse.com

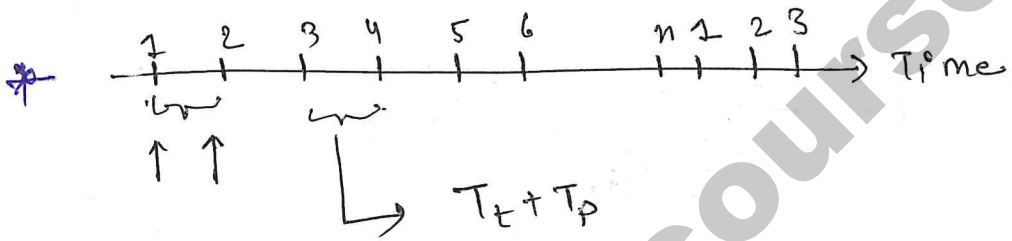
APPLIED COURSE
Ph: +91 844-844-0102

Time division multiple access:-



→ We are dividing the time into intervals.

→ In each interval we are giving turn to various hosts.



* assume all packets are of same size.

$$\eta = \frac{T_t}{T_t + T_p} = \frac{1}{1+a} \qquad a = \frac{t_p}{t_t}$$

$$\text{Throughput} = \eta \times B.$$

Drawback of TDM:-

* There are instances where some hosts or stations don't want to transmit data then that particular slot will be idle and no. transmission of data takes place

$$\eta = \frac{T_t \times 3}{4(T_t + T_p)}$$

→ This is not sending

→ Efficiency reduced

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que: $T_t = 1\,ms$

$T_p = 1\,ms$ ← TDMA

(a) $\eta = ?$ (b) $B = 4\,Mbps$

Throughput / available-BW =>

(c) If every station / host needs 1Mbps bandwidth, No. of stations that can be connected.

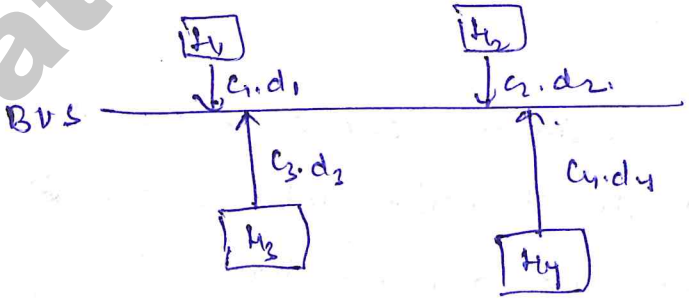
Soln:

(a) $\eta = \frac{1}{1 + (T_p/t_t)} = \frac{1}{1+1} = 50\%$

(b) $\eta \cdot B = 2\,Mbps$

(c) $\frac{2 \times 10^6\ bps}{1 \times 10^3\ bps} = 2000$

Channelization: code division multiple access (CDMA)



Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

$$c_1 \cdot d_1 + c_2 \cdot d_2 + c_3 d_3 + c_4 \cdot d_4 \cdot = \sum_{i=1}^{4} c_i d_i$$

→ Here we are putting data together in the medium.

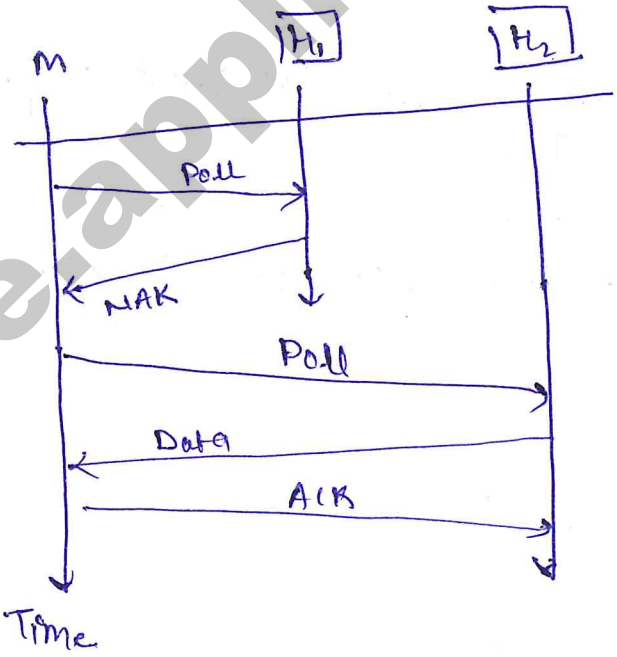
→ We can decouple data d_1, d_2, d_3, d_4 because we know what c_1, c_2, c_3, c_4 are.

CDMA → Used by Reliance Telecomm

Polling, Reservation, Token Passing

Polling: M: master / controller / primary

Common topology: STAR. → In case of polling



1, 2, 3 ... n ... 1, 2 ... order

In a polling mechanism, master Poll the host 1. If host 1 sends the data it will send Data. Otherwise it send NAK frame and similarly master poll host 2 and so on.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

→ Poiorittzations

Let suppose we want to poiorittze host 1

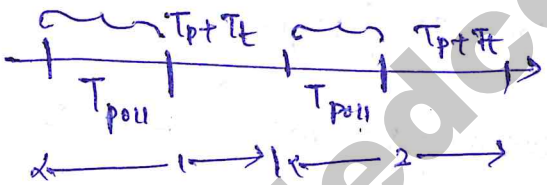
So, we will go like 1, 2, 1, 3, 1, 4- - - -

After some time we are recalling one.

→ Band wiath utilisation is low in polling

→ Single point of feilure means if master fails everything fails.

Timings →



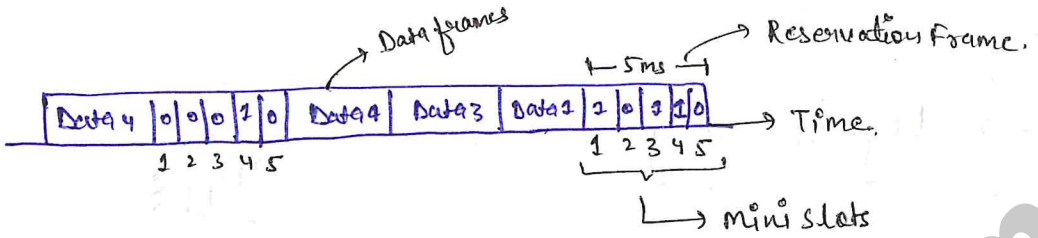
$$\eta = \frac{T_t}{T_t + T_p + T_{poll}}, \quad \text{Throughput} = \eta \cdot B$$

* Efficiency is lower, so BW is lower.

Gate.appliedcourse.com
gatecse@appliedcourse.com

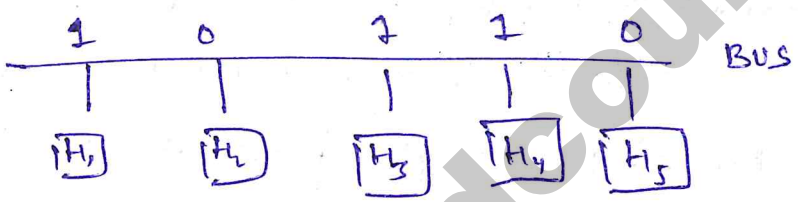
APPLIED COURSE
Ph: +91 844-844-0102

Reservation :-



In this approach we are putting the reservation frame on the channel.

Each host we are providing 1ms to put their reservation bit



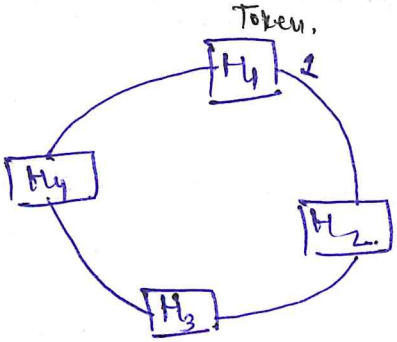
* Now we have default order H_1, H_2, H_3, H_4, H_5 and each host got to know who will send the data first.
* Accordingly H_1 place $Data_1$, Now H_3 place $Data_3$, and H_4 place $data_4$.
* When data-transfering is done we again put the reservation frame on the channel.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Token - Passing / Ring :-

→ Logical ring



→ Token : whoever have a token has a permission to transmit

→ No Ack is required because once the packet starts moving in the ring. The destination took that packet and again forwards in the ring. Once the packet reaches to ~~host 1~~ the source again. It got to know that transmission completed sucessfully.

→ Packet removal will be done by source itself.

→ When transmission is completed and source now can send the token on the ring.

→ Using ring topology broadcasting can be done very efficiently.

Concept → B-bit delay.

B : 1 sec → B bits
V : 1 sec → V mtrs.

Ex→ K-bit distance.?, Bandwidth = B bits/sec,

Soln→ 1 sec = B bits

1 bit = $1/B$ sec

K bits = K/B sec = $K/B \times V$ = KV/B metres.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Mathematics of token ring:

n - stations / hosts
d = distance (m)
v = velocity (m/s)

B : Bandwidth (bps)
k : delay @ each station in bits.

$$\text{ring Latency} = \left(\frac{d}{v} + \frac{n \cdot k}{B}\right) \text{sec}$$

$$= \left(\frac{dB}{v} + nk\right) \text{bits}$$

$$= T_p + \text{bit-delay}$$

↳ often time we take this as zero.

Token holding time :- (THT)

* The time each hosts hold the token.

Cycle time: $\left(\frac{d}{v}\right)_{T_p} + (n * THT)$

$$\eta = \frac{\text{Useful time}}{\text{Cycle time}} = \frac{n \times T_t}{\left(\frac{d}{v} + n(THT)\right)}$$

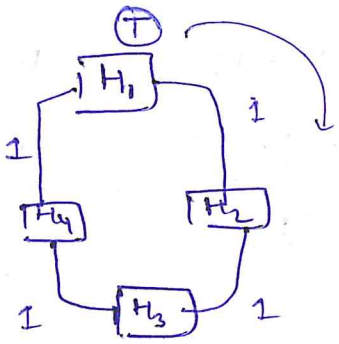
Assume: Each station sends exactly one frame.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

THT (Delayed-token reinsertion)

→ Token held till it returns to the token holder



Only one packet at a time on the ring

$$THT_{DTR} = T_t + RL$$

$$\eta_{DTR} = \frac{\eta T_t}{\frac{d}{V} + \eta (T_t + RL)} = \frac{\eta T_t}{T_p + \eta \left(T_t + T_p + \frac{\eta K}{B}\right)}$$

Let K=0 bit delay

$$= a = \frac{T_p}{T_t}$$

$$\eta_{DTR} = \frac{1}{1 + \left(\frac{n+1}{n}\right) a}$$

⇒ Efficiency of Delayed token reinsertions

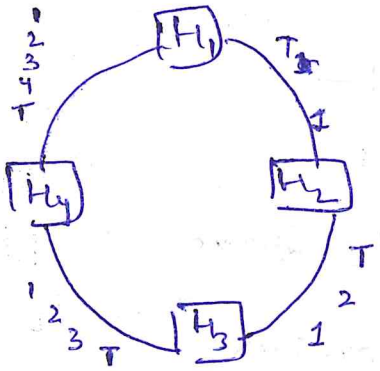
Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

THT (Early-token-reinsertion)

$THT_{ETR} = T_t$ [Assuming bit-delay 0]



Multiple packets @ same time on the ring

$$\eta = \frac{n \cdot T_t}{T_p + \eta(T_t)}$$

* $\eta_{ETR} = \frac{1}{1 + a/n} > \eta_{DTR}$ =

→ More efficiency and lower reliability.

* Here after sending a packet every host sending a token also onto the ring.

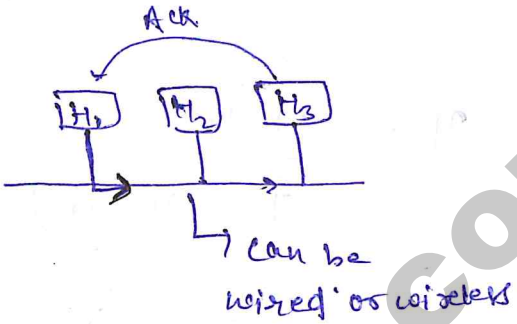
* In ETR corruption of data will be more as compared to DTR.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Random - Access - Protocol: Aloha. [Univ of Hawaii] → It is designed for wireless comm.

Pure Aloha :—



→ Just send the frame

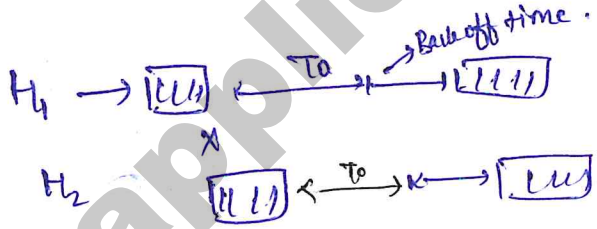
→ Ack from receiver

→ Collisions

→ Retransmit after random backoff time.

* Whenever you have a packet just send it without thinking of anything in pure aloha.

* chances of collisions more we are not waiting for anything.



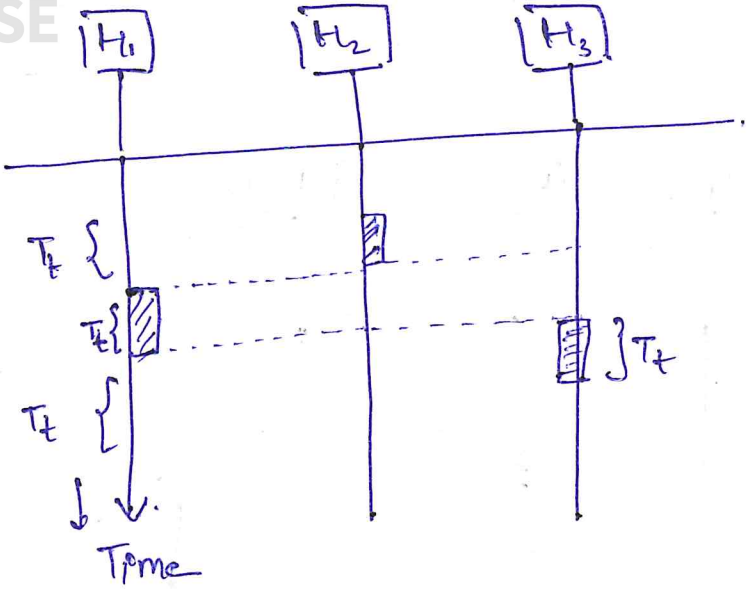
* We are using back-off algorithm for the re-transmission.

Vulnerable time (T_v) = $2 \times T_t$

* The time where the possibility of collision.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102



* $\eta_{PA} = G \cdot e^{-2G}$ [Poisson's distribution].

G = No. of hosts that want to transmit

To maximize the efficiency we have to take derivative zero.

$$\frac{d\eta_{PA}}{dG} = 0$$

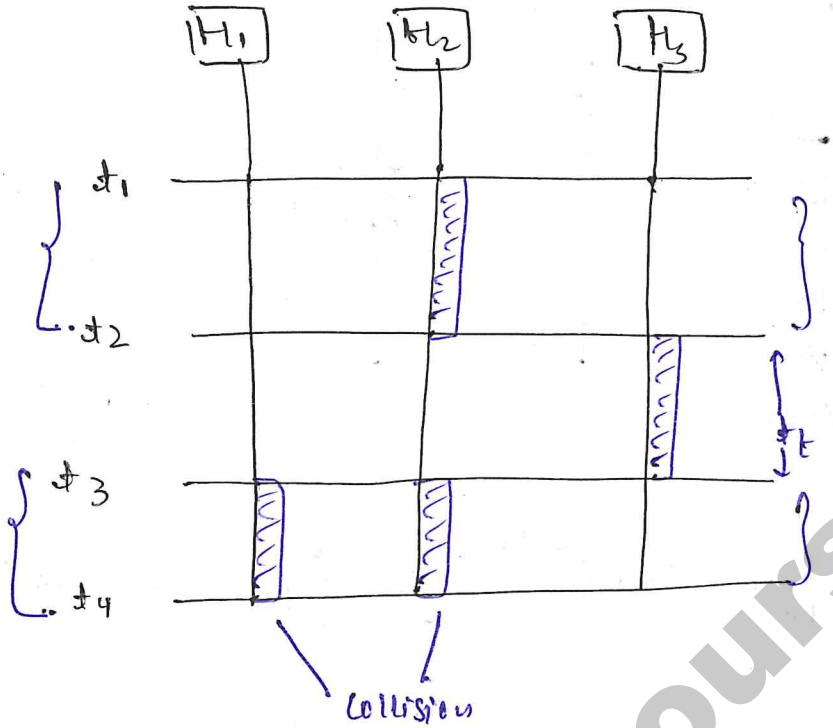
$G = 1/2 \Rightarrow \eta_{PA}^{MAX} = 0.184 = 18.4\%$.

* Maxm efficiency of pure aloha is 18.4%.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Slotted Aloha:-



→ Vulnerable time = T_t

→ Here we are breaking the whole time axis every gap is equal to T_t.

→ Any station can transmit only start of the time slot.

* $\eta_{SA} = G e^{-G}$

Max $\eta_{SA} \Rightarrow G = 1$

$\Rightarrow \eta = 1/e = 0.368 = 36.8\%$.

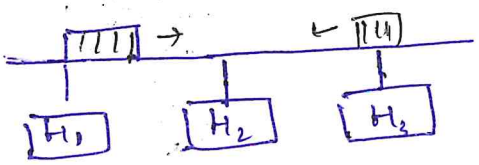
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

CSMA : Carrier-sense multiple access :-

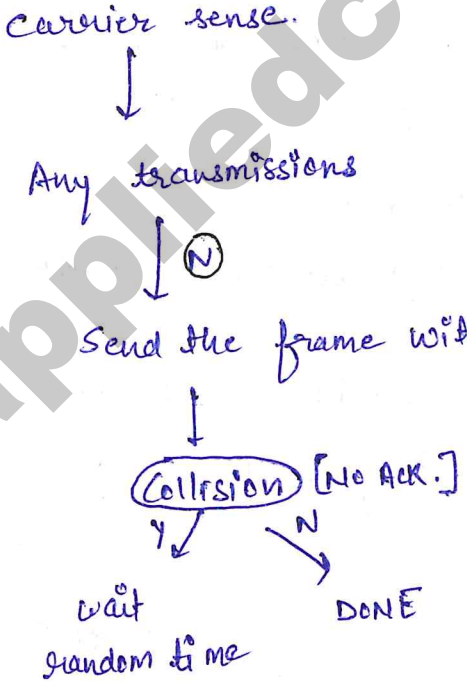
1 - persistent CSMA :

* collisions due to T_p
* Small T_p in real word (better than Aloha).
[Ethernet LAN]



→ It first senses the channel and whenever the channel is ideal. It will transmit with probability = 1.

→



Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Non-Persistent CSMA :—

→ Less greedy {whenever find any packet on the medium just wait for random amount of time}
→ longer delay than 1-persistent.

P-Persistent CSMA

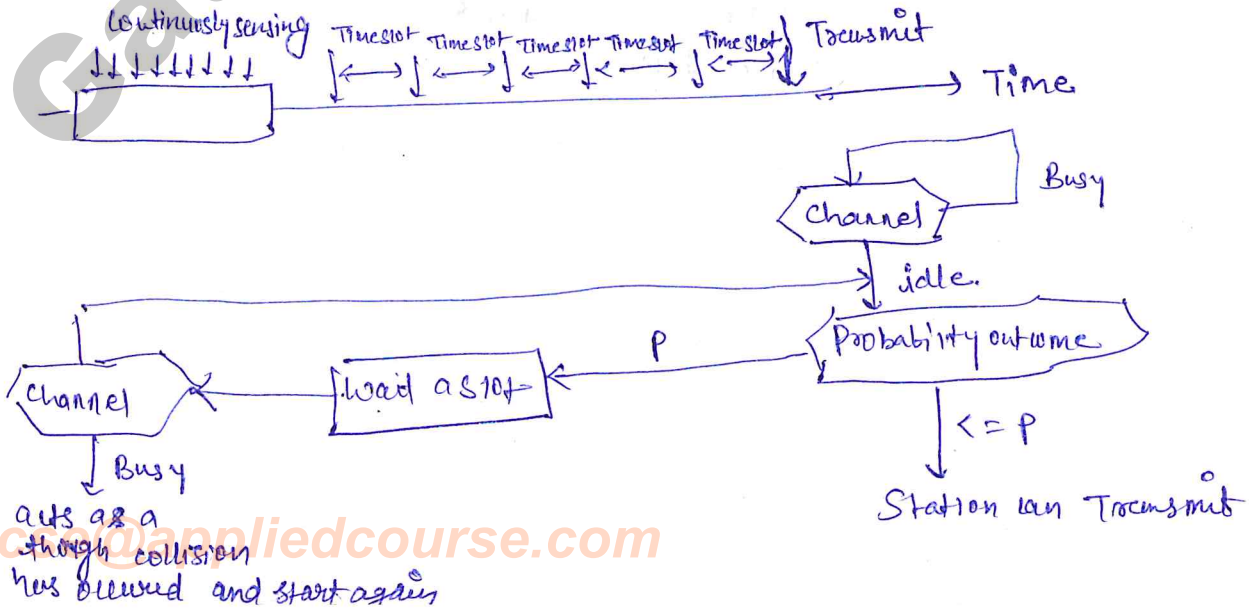
→ Used in wireless LANs
→ Slotting [concept of slotting]

Step-1 It keeps sensing the channel and busy.

Step-2 Once the channel is idle it generates the random variable $0 \le r \le 1$

if $r < p$ → Transmits
$r > p$ → wait for a slot → After sense the channel.

* When channel is idle it will transmit with probability p and not transmit with probability 1-p.



gatecse@appliedcourse.com

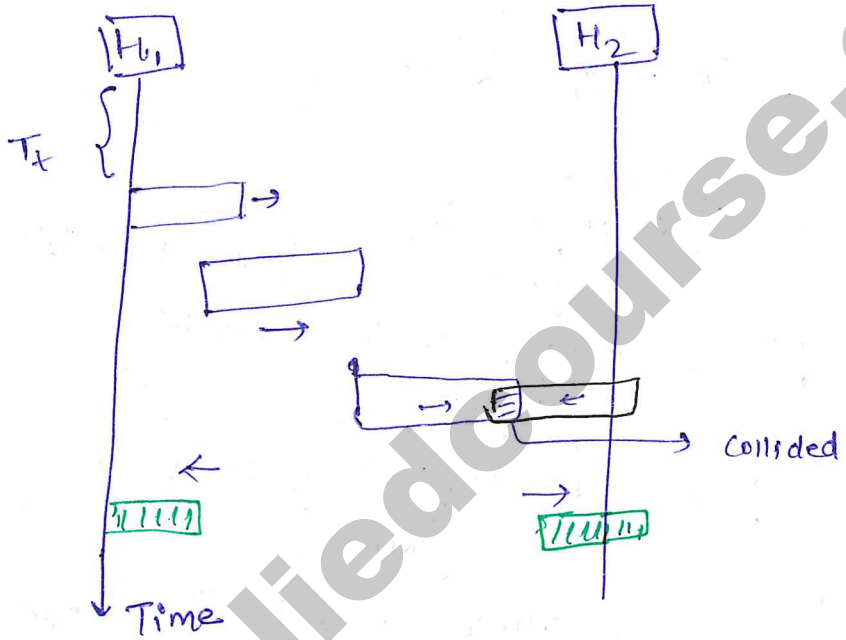
APPLIED COURSE
Ph: +91 844-844-0102

CSMA/CD :— (collision-detection)

→ No-ACK-needed.

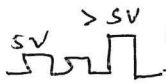
→ { Collision detection } media-dependent

(a)



* Here Packet of H_1 and H_2 get collided the H_1 and H_2 will received the corrupted data.

(a) Compare sent and received state. } → we use to find CD

(b) high signal amplitude. ← dependent] → 

when any signal receive with more amplitude

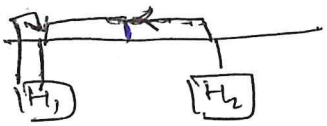
(c) receiving signal while still transmitting

↳ common approach.

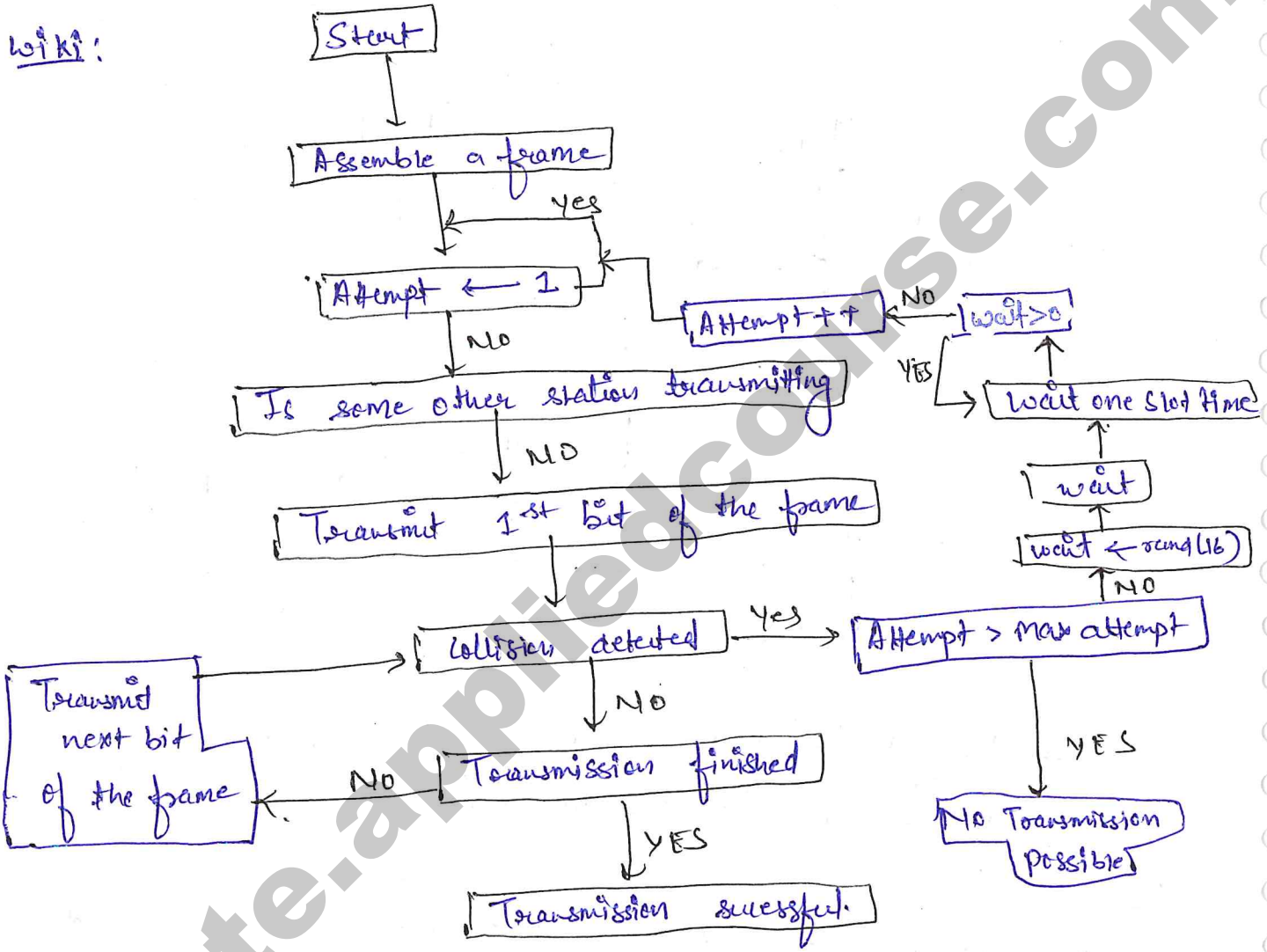
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

We can analyze the signal when we are transmitting.



Wiki:

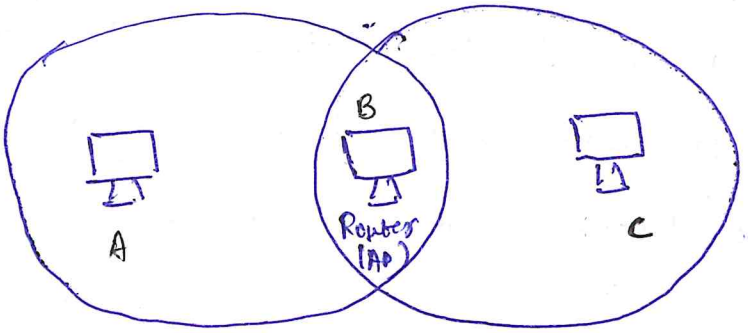


Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

CSMA/CA : Collision avoidance [wireless LAN IEEE 802.11]

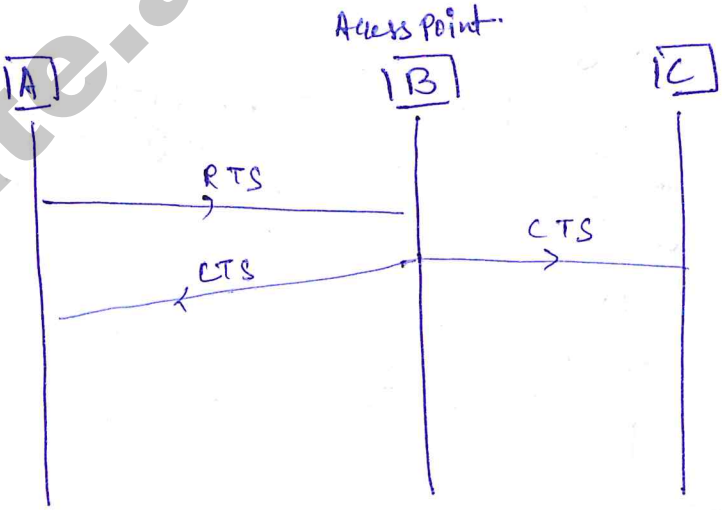


Hidden-node problem.

* A is not in range of C.
* When C is transmitting data, A doesn't know that C is transmitting.

* Hidden node problem is very particular to csmA' wireless.
* We use RTS/CTS exchange to solve the hidden node problem.

RTS → Request to send.
CTS → clear to send.

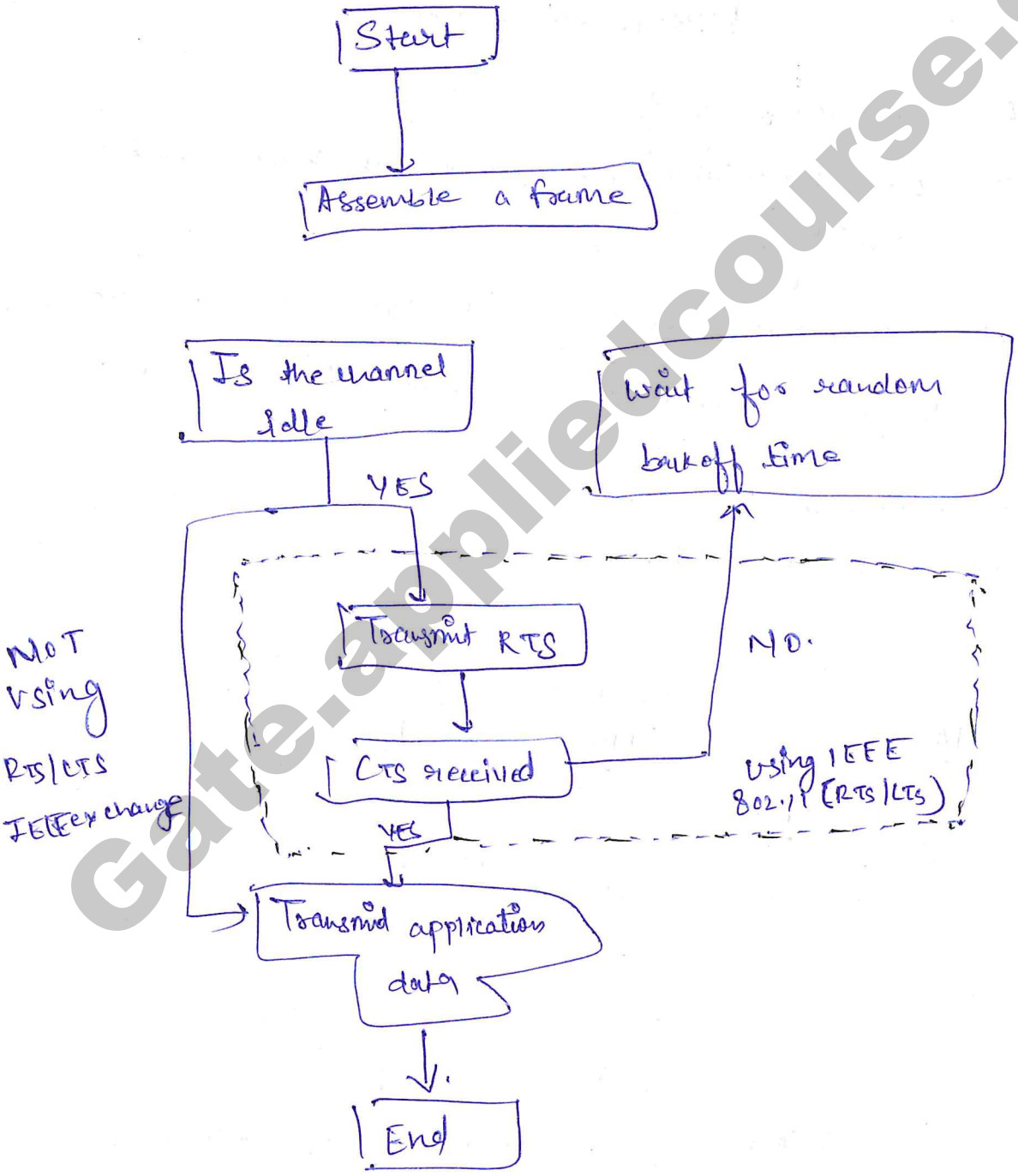


* Here node A send RTS request to node B. Node B send the CTS to A. So this A will

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

start transmitting the data to B. The CTS will also reach to node C. That is why C also knows that someone is transmitting to B and C will wait for some time before sending RTS to B. This solves the hidden node problem.

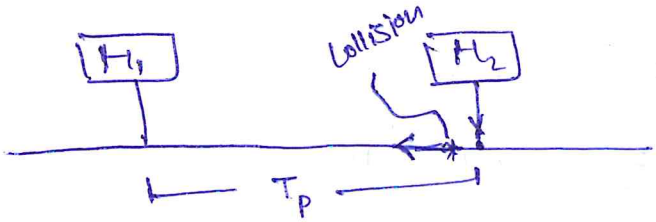


Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

CSMA/CD analysis and efficiency:

CD: receving signal while transmitting



* Let suppose collision takes place just few dist near to host 2. The collision happens at propagation time.
* The collision signal reaches again (T_p time) takes to reach H_1.

To detect the collision.

$$T_t \geq 2T_p$$

$$\Rightarrow L/B \geq 2T_p$$

$$\Rightarrow L \geq 2T_p B$$

$$\Rightarrow \boxed{L \geq 2\frac{d}{V}B}$$

minimum size of frame to detect the collision.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Eg $T_p = 1ms$

$B_w = 1 Mbps$

min L for CD = ?

Soln $L \geq 2T_p \cdot B$

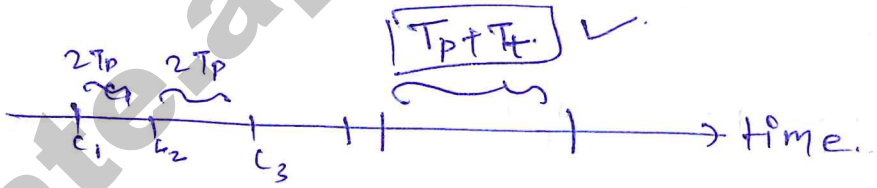
$\min L = 2T_p \cdot B$

$\min L = 2 \times 10^6 \times 10^{-3}$

$= 2000 bits.$

$\eta_{CSMA/CD}$:- Time wasted due to one collision $= 2T_p$ (worst case)

$$\frac{UT}{TT} = \eta = \frac{T_t}{2T_p l + T_t + T_p}$$



* Here c_1, c_2, c_3 representing no. of collisions in the time axis.

η_t

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Assume: Only one station transmitting @ a time.

P = Probability that a stations transmits.

Probability of success ← $P_S = {}^{n}C_1 \cdot p \cdot (1-p)^{n-1} = n \cdot p \cdot (1-p)^{n-1} = f(p, n)$

Max P_S $\quad \frac{\partial P_S}{\partial p} = 0 \Rightarrow p = 1/n$

$\Rightarrow P_S^{max} = n \cdot 1/n \, (1-1/n)^{n-1}$

$\lim_{n \to \infty} P_S^{max} = 1/e.$

* If we have large number of stations the maximum probability of station $P_S^{max} = 1/e.$

Ex→ Number of times we have to try before successfully transmitting.

Soln→ $P_S^{max, n \to \infty} = 1/e.$

⇒ 1 success in e trails

Expected value of $C = e.$

Gate-appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

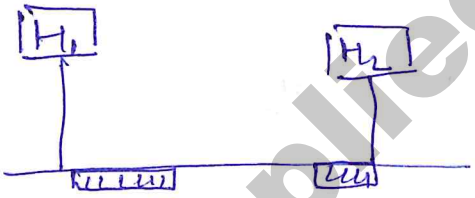
Now,

$$\eta_{(CSMA/CD)} = \frac{T_t}{2 \cdot e \cdot T_p + T_p + T_t} = \frac{1}{1 + 6.44a}$$

$$= \frac{1}{1 + 6.44\left(\frac{d}{v} \times \frac{B}{L}\right)}$$

$\uparrow \eta$ vs $L\uparrow$ or $\int \eta$ vs $d\uparrow$

Exponential back off Algorithm: →



One → How long to wait once we detect a collision?

Waiting time = Back off time.

* Both the hosts should wait for random amount of time.

waiting time = $W = K \times T_{slot}$

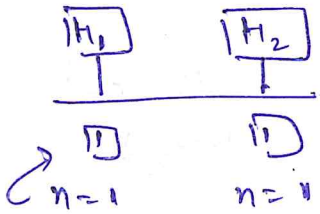
K: Choosen randomly.

Gateappliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Case - 1



$P(C_1) = 1$

* Both of the hosts collided for the first time

The random number H_1 will wait and H_2 will wait

$= [0 \text{ to } 2^n - 1] \Rightarrow$ For first time. collision $n = 1$

H_1	H_2	
0	0	$\rightarrow C_2$ [second time collision]
0	1	$\rightarrow H_1$ success
1	0	$\rightarrow H_2$ success
1	1	$\rightarrow C_2$

$P(C_2/C_1)$ = probability of collision 2 after collision 1 $= \frac{2}{4} = \frac{1}{2} = 0.5$

$P(H_1/C_1)$ = Host 1 successfully transmits after collision 1 $= \frac{1}{4} = 0.25$

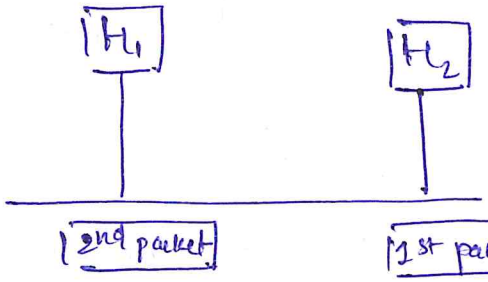
$P(H_2/C_2)$ = Host 1 successfully transmits after collision 1 $= \frac{1}{4} = 0.25$

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Case-2 For the first time collision-1 takes place.
For the second time Host 1 successfully transmitted

Now, Host 1 is sending 2nd packet and Host 2 is sending 1st packet and collision 2 happens.



$n = 1$

$n = 2$ → because second time it get collided

$[0 \text{ to } 2^n - 1]$

$n = 1$

$= (0, 1)$

H_1

0
0
0
0
1
1
1
1

$[0 \text{ to } 2^n - 1]$

$n = 2$

$(0, 1, 2, 3)$

H_2

0 → C_3
1 → H_1 wins
2 → H_1
3 → H_1
0 → H_2
1 → C_3
2 → H_1
3 → H_1

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

$P(H_1/C_2) = 5/8$

$P(H_2/C_2) = 1/8$

$P(C_3/C_2) = 2/8 = 1/4$

* Using the Exponential back off the probability of 2nd collision after 1st collision will decrease.

Capture Effect:

* Winning hosts have the highest probability of winning again.

Solution: Use collision free algorithm : Token Passing

SOLVED PROBLEMS FROM GATE:

Que: The values of parameters for the stop and wait ARQ protocol are as given below:

Bit rate of the transmission channel = 1 Mbps

Propagation delay from sender to receiver = 0.75 ms.

Time to process a frame = 0.25 ms

Number of bytes in the information frame = 1980

Number of bytes in the acknowledge frame = 20

Number of overhead bytes in the information frame = 20

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Assume that there are no transmission errors. Then the transmission efficiency (expressed in percentage) of the stop and wait ARQ protocol for the above parameters is ____ (correct to 2 decimal places).

Soln: $B_W = 1$ Mbps $T_P = 0.75$ ms

$T_{pr} = 0.25$ ms

$$\eta = \frac{UT}{\text{Total time}}$$

⇒ Number of bytes in information frame = 1980

⇒ Overhead bytes = 20

∴ actual data = 1980 − 20 = 1960

$$TT = DS/B_W = \frac{1960 \times 8}{10^6} = \text{Useful time} = 15.68 \text{ ms}$$

Overhead bits $TT = 0.16$ ms.

$$\eta = \frac{UT}{TT} = \frac{15.68}{15.68 + 0.16 + 0.75 + 0.25 + 0.16 + 0.75 + 0.25}$$

15.68 + 0.16 → TT including overhead; +0.75 → PT; +0.25 → Pr; +0.16 → TT ACK; +0.75 → PT ACK; +0.25 → PT ACK

$$\eta = \frac{15.68}{\text{Total}} = 87\%$$

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que.2 A network has a data transmission bandwidth of 20×10^6 bits per second. It uses CSMA/CD in the MAC layer. The maximum signal propagation time from one node to another node is 40 microseconds. The minimum size of a frame in the network is ____ bytes.

Ans → $Bw = 20 \times 10^6$ b/s , $PT = 40 \times 10^{-6}$ s

$$T_t \geq 2T_p$$

$$\min T_t = 2T_p$$

$$L/B = 2 \times 40\ \mu s$$

$$\min L = 2 \times 40 \times 10^{-6} \times 20 \times 10^6$$

$$= 1600 \text{ bits} = 200 \text{ B}$$

Que Consider a LAN with four nodes S_1, S_2, S_3 and S_4. Time is divided into fixed size slots, and a node can begin its transmission only at the beginning of a slot. A collision is said to have occured if more than one node transmit in the same slot. The probabilities of generation of a frame in a time slot

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

by S_1, S_2, S_3 and S_4 are 0.1, 0.2, 0.3 and 0.4, respectively. The probability of sending a frame in the first slot without any collision by any of these four station is ____.

(A) 0.462
(B) 0.711
(C) 0.5
(D) 0.652.

Ans: $\underbrace{0.1\,(0.8)\,(0.7)(0.6)}_{S_1} + \underbrace{0.9\,(0.2)\,(0.7)\,(0.6)}_{S_2}$

$\Rightarrow$

$+\underbrace{(0.9)\,(0.8)\,(0.3)\,(0.6)}_{S_3} + \underbrace{(0.9)\,(0.8)\,(0.7)\,(0.4)}_{S_4}$

$\Rightarrow$ 0.462.

Que Consider a CSMA/CD network that transmits data at a rate of 100 Mbps (10^8 bits per second) over a 1 km (kilometre) cable with no repeaters. If the minimum frame size required for this network is 1250 bytes, what is the signal speed (km/sec) in the cable?

(A) 8000 (B) 10000 (C) 16000 (D) 20000

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Sol. $d = 1$ km $\quad B = 10^8$ bps $\quad L = 1250 \times 8$ b

$$T_t \geq 2 T_p$$

$$\Rightarrow \quad L/B \geq 2 \cdot d/v$$

$$\Rightarrow \quad \min L = 2\, d/v \times B$$

$$1250 \times 8 = 2 \times \frac{1}{v} \times 10^8 \text{ bps}$$

$$v = \frac{2 \times 10^8}{8 \times 1250} = \frac{10^8}{5 \times 10^3} = \frac{10^5}{5} = 2 \times 10^4 = 20{,}000$$

Que. A sender uses the stop and wait ARQ protocol for reliable transmission of frames. Frames are of size 1000 bytes and the transmission rate at the sender is 80 Kbps (1 Kbps = 1000 bits/second). Size of an acknowledgement is 100 bytes and transmission rate at the receiver is 8 Kbps. The one way propagation delay is 100 milli seconds. Assuming no frame is lost, the sender throughput is ____ bytes/second.

Sol:

$$L = 1000 \times 8 \text{ b}$$

$$B_S = 80 \times 10^3 \text{ bps} = 10 \text{ KB}$$

$$\text{ACK} \rightarrow 100 \times 8 \text{ b} = 100 \text{ B}$$

$$B_R = 8 \times 10^3 \text{ bps} = 10^3 \text{ B/s}$$

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Throughput $= \eta \times B_s$

$$\eta = \frac{UT}{TT} = \frac{0.1}{0.1+0.1+0.1+0.1} = \frac{0.1}{0.4} = \eta_4 =$$

$$= 1/4 \times 10,000 = 2500 \text{ B/s}$$

Que Consider a 128×10^3 b/sec satellite communication link with one-way propagation delay of 150 milli seconds. Selective retransmission (repeat) protocol is used on this link to send data with frame size of 1 Kilobyte. Neglect the transmission time of acknowledgement. The minimum number of bits required for the sequence number field to achieve 100% utilization is.

(A) 2 (B) 4 (C) 6 (D) 8

Ans :- $T_p = 150 \text{ ms}$ $l = 1 \text{ KB}$

$$\eta = \frac{W_s}{1+2a} = 100\%$$

$$T_t = \frac{1 \times 8 \times 10^3}{128 \times 10^3} \text{ sec}$$

$$W_s = 1+2a$$

$$\Rightarrow 1 + 2\frac{T_p}{T_t}$$

$$W_s = 5.687 \simeq 6$$

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

$W_S = W_R = 6$

min sequence numbers $= 2N = 12$

For 12 sequence number = we need 4 bits.

Ans = 4.

Que Suppose that stop and wait protocol is used on a link with a bit rate of 64 Kilo bits per second and 20 miliseconds propagation delay. Assume that the transmission time for the acknowledgement and the processing time at nodes are negligible. Then the minimum frame size in bytes to achieve a link utilization of at least 50% ____.

(A) 160 (B) 320 (C) 640 (D) 220

Sol. $B = 64$ Kbps $T_p = 20$ ms

min $\eta = 50\% = 1/2 = \frac{UT}{TT}$

$= \frac{L/64\text{ Kbps}}{L/64\text{ Kbps} + 20\text{ms} + 20\text{ms}} = 1/2.$

$\Rightarrow 1/2\left(L/64 + 40\right) = L/64$

$L/128 + 20 = L/64 \Rightarrow L/128 = 20$

$\therefore L = \frac{128 \times 20}{8} = 320$ bytes.

Gate-appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que: A link has a transmission speed of 10^6 bits/sec. It uses data packets of size 1000 bytes each. Assume that the acknowledgement has negligible transmission delay, and that its propagation delay is same as the data propagation delay. Also assume that the processing delays at nodes are negligible. The efficiency of the stop and wait protocol in this setup is exactly 25%. The value of the one way propagation delay (in milliseconds) is

(A) 4 (B) 8 (C) 12 (D) 16

Sol: $B = 10^6$ bps $L = 1000 \times 8$ b $T_p = ?$

$$T_t = \frac{1000 \times 8}{10^6} = 8 \text{ msec}$$

$$\eta = \frac{1}{4} = \frac{UT}{TT} = \frac{8ms}{8 + T_p + T_p}$$

$$\frac{1}{4} = \frac{8}{8 + 2T_p} \Rightarrow 2T_p = 24$$

$$T_p = 12$$

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que. Consider a network connecting two systems located 8000 Kilometers apart. The bandwidth of the network is 500×10^6 b/s. The propagation speed of the media is 4×10^6 meters per second. It is needed to design a Go-back N sliding window protocol for this network The average packet size is 10^7 bits. The network to be used to its full capacity. Assume that the processing delays at nodes are negligible. Then, the minimum size in bits of the sequence number field has to be.

(A) 2 (B) 4 (C) 8 (D) 16

Ans: $d = 8000$ km, $B = 500 \times 10^6$ bps $V = 4 \times 10^6$ mps

$l = 10^7$ bits

$$\eta = 1 = \frac{w_s}{1+2a} \Rightarrow 1 + \frac{2T_p}{T_t} = w_s$$

$$T_p = \frac{d}{v} = 2 \quad , \quad T_t = l/B = \frac{10^7}{50 \times 10^7} = \frac{1}{50}$$

$$w_s = 1 + (2 \times 2 \times 50) = 201$$

No. of sequence no $= w_s + 1$

$= 202$

No. of bits $= \log_2 202 = 8$ bits.

Gate.appliedcourse.com
gatecse@appliedcourse.com

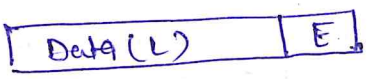
APPLIED COURSE
Ph: +91 844-844-0102

Error-handling in MAC Layer.

- Detection
  - Parity (DLD)
  - CRC
  - Checksum
- Correction
  - Hamming code
  - Convolution-code

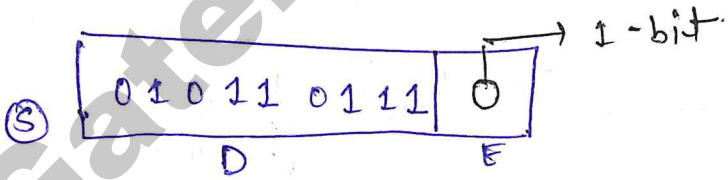
wiki ↑

* We are going to focus on error detection much.



E → Error detection bits E << L

PARITY :— Even zero parity

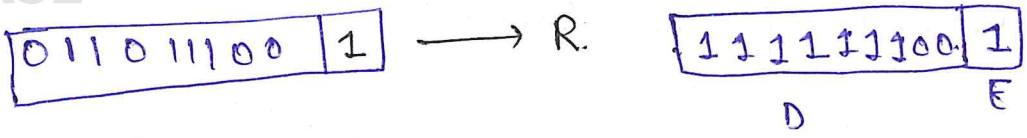


Here we want to make the number of zeroes to be even.

* If Receiver find odd zeros than there is error.
  If receiver find even zeros than not sure there is error.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

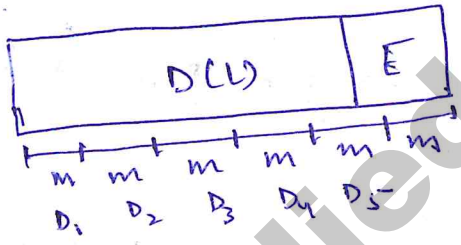


even zero's

→ Here at the receiver end if two bit change happen. The receiver think it is of even parity and accepted the corrupted data.

* cannot handle / detect errors in 2-bits or more.

Checksum :-



$$E = f(D_1, D_2, \cdots D_5)$$

Ist strategy : function is addition

$$E = D_1 + D_2 + D_3 + \cdots D_5$$

IInd strategy :

$$E = D_1 + D_2 + \cdots D_5 + c(D_1 + D_2 + \cdots D_5)$$

* Here in this method we are adding error detection bits in the last of data. We are performing some operation on data to get the error detection bits. The same thing is repeated by the receiver when it gets the data.

Gate.appliedcourse.com
gatecse@appliedcourse.com

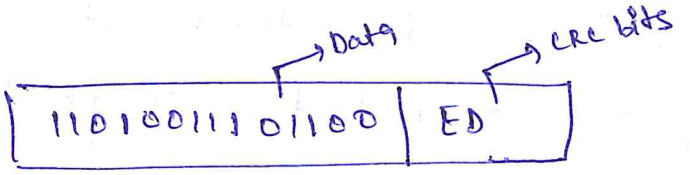
APPLIED COURSE
Ph: +91 844-844-0102

Cylic Redundancy check (CRC)

→ Uses division

→ based on Galois fields (GF)

Ex →



$x^3 + x + 1$ → Galois field polynomial / CRC polynomial.

* Sender and receiver both agree upon the CRC bits.

* If CRC bit = 3 than largest exponent is also three.

So, $x^3 \cdot 1 + x^2 \cdot 0 + x \cdot 1 + 1 \cdot 1 = x^3 + x + 1$

Divisor = 1011.

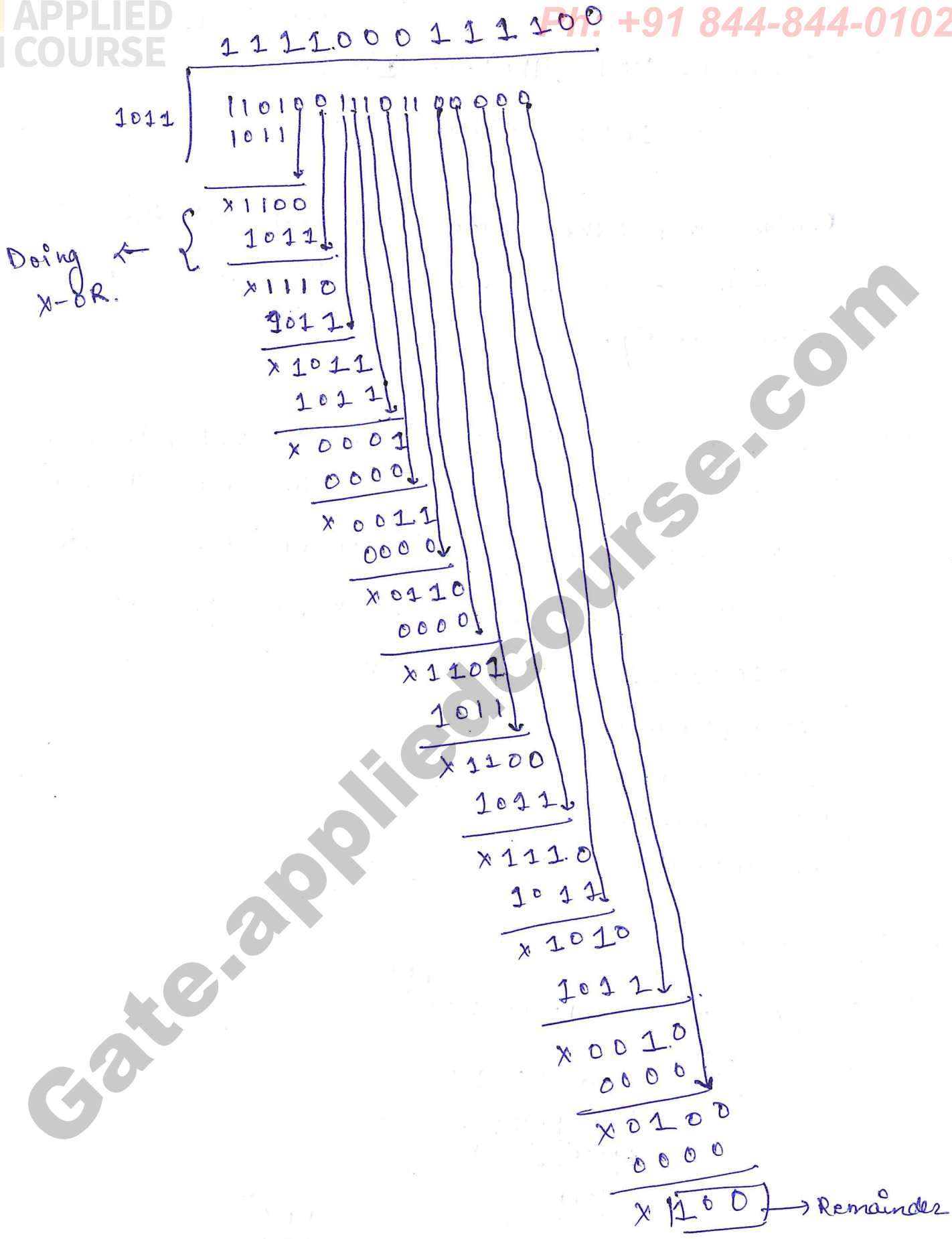
* Since we are using three bits CRC we have to add three zero's in data.

1101001111011 00 [000] ← Three additional bits

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
PH: +91 844-844-0102



Gate.appliedcourse.com

* Now we ~~send~~ replace the remainder with three zero's and send to the sender.

gatecse@appliedcourse.com

APPLIED COURSE
Ph: 191 844-844-0102

So, Sent data = 1101001110111 00 | 100 → CRC bits calculated.

1011 → divisor

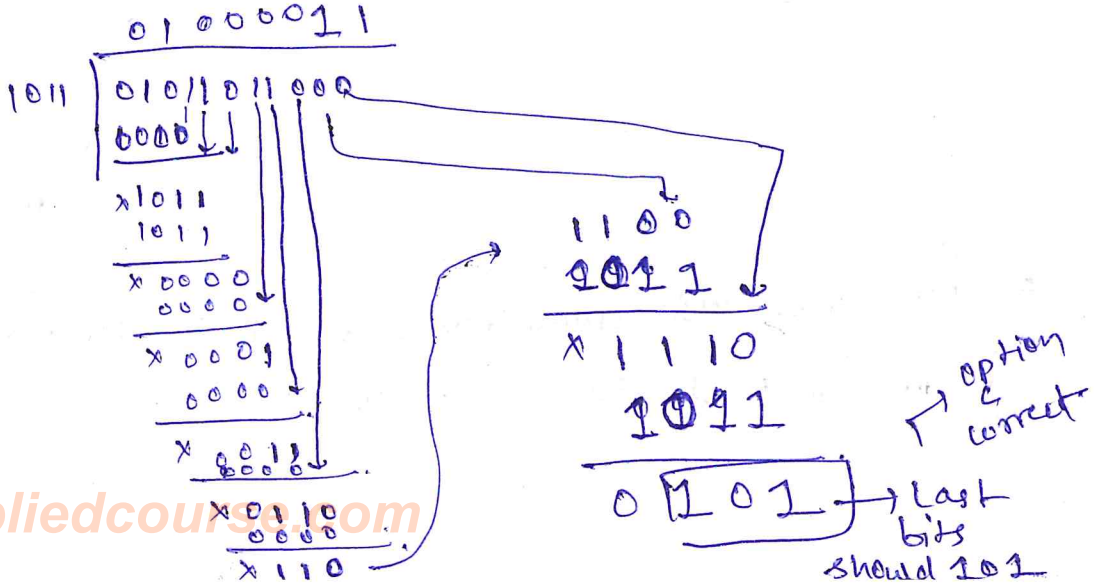
Receiver repeat the same step and get the remainder zeros in the last. This means data sent correctly.

Que: A computer network uses polynomial over GF(2) for error checking with 8 bits as informations bits and uses x^3+x+1 as the generator polynomial to generate the check bits. In this network, the message 01011011 is transmitted as

(A) 010110110 10
(B) 010110111 01
(C) 010110111 01
(D) 010 110111 00

Sol: x^3+x+1 = 1011

message = 01011011 000 ← CRC



Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Framing

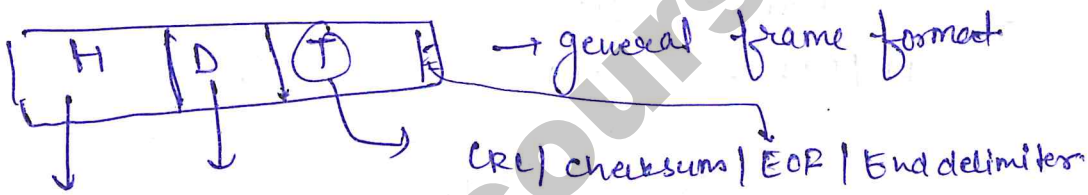
Network - layer (Packet)

↓

DLL (FRAME)

↓

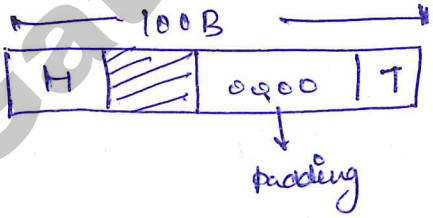
Physical layer



Frame no.
Size
protocol
SOF
Sender mac address
Receiver mac address

Packet from network layer.

Fixed size framing



* It wastes the space some time because we always need to follow some size.

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Variable-sized framing

→ length (Ethernet)

→ EOF (Token-ring) / end-delimiter

Problem → What if end-delimiter occurs in the data part ?

Data = 01111

ED / EOF = 01111

Sender → | Data: 01111 | ED: 01111 |

So, receiver can think 'Data as ED because both ED and data are same.

To handle this problem we are using bit stuffing.

* In bit stuffing we are stuffing 0/1 based on the ED

ED = 01111 ⇒ we make a rule that after every three one's we will stuff '0' in data part.

So, Now data = 01110 1 01111

(Data: 01110 ; ED: 01111 ; bit stuffing)

gatecse@appliedcourse.com
Gateappliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Ex→ A-bit-stuffing based framing protocol uses 8-bit delimiter pattern of 01111110. If the output string after stuffing is 011111100101, then the input string is?

Ans: ED → 0 111 111 0] → We will stuff zero after 5 one.

Remove ↓

O/p after stuffing : 0 1111 1 00 1 0 1

↳ Remove zero after 5 one.

Actual data = 0 11111 0 1 0 1

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

LAN-Protocols : Ethernet, Token ring, WLAN.

(I) Ethernet : IEEE 802.3

→ Constantly evolving (wiki): 2.94 Mbps, 10Mbps, 100 Mbps, 1Gbps, 25Gbps, ...

→ Bus Topology

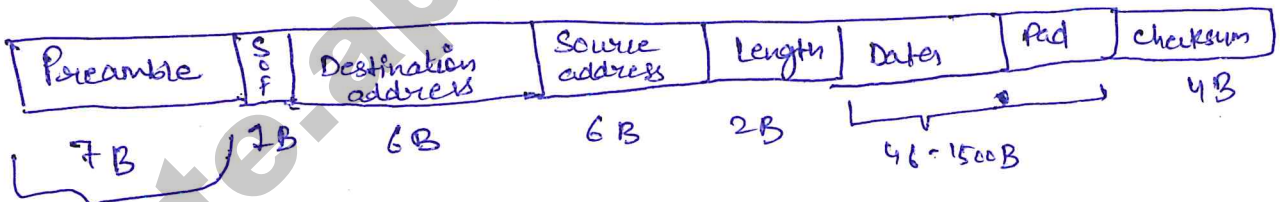
→ CSMA/CD ⇒ No ACK. [MAI]

→ Manchester encoding [Physical-Layer]

→ Expo. backoff algorithm.

* Twisted cable / Co-axial cable / fibre optical

FRAME-format (802.3)



10 1010 1011

* Preamble and sof are generally not considered as part of frame.
* Preamble and sof are added by the physical layer.
* Preamble is sending a clock signal to synchronize the receiver.
* SOF is the starting of frame.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

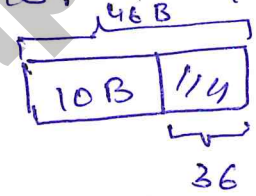
* Destination and source address are the MAC address which are of 6B = 48 bit

6B = 48 bits = 12 Nibbles

1 Nibble = 4 bits → 0 .... 9, A ... F

* MAC address are represent using a hexadecimal symbol.
* Length field tells us about the length of frame excluding preamble and SOF.
* Max size of frame = 1518 B
  Min Size of frame = 64 B

Concept → If your minimum data size is 10B in the frame. Then you have to add 36B padding to make it to 46 B.



* We are limiting the maximum size of frame is 1518 because. if we didn't set the upper limit then all other users will get blocked.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

→ Protocol efficiency = $\frac{\text{Pay-load size}}{\text{Packet size}}$ = $\frac{1500}{1518}$ = 98.81 %.

→ condition for CD : $L \geq 2 \cdot \frac{d}{v} \cdot B \Leftarrow TT \geq 2T_p$.

→ collision vs real time applications

↳ max time to transmit successfully

→ real time applications [video calls, Youtube live]

In real time application we expect less errors.

Token - Ring (802.5)

→ Encoding : Diff manchester.

→ Token-passing ⇒ No collisions, No ACK.

→ 4Mbps, 16Mbps, 1 Gbps

→ Prioritization and server - client architectures.

* In token ring we need a logical ring topology.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

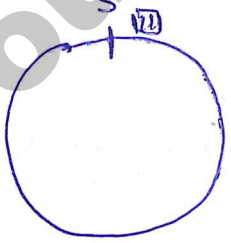
* If any host has the higher priority for holding the token then the token holding time for that host is more as compared to other hosts.

* In token ring there is no collisions and no Ack so we know exact time for the frame transmission. It is feasible to design real-time application using token ring.

Dis-advantages:-

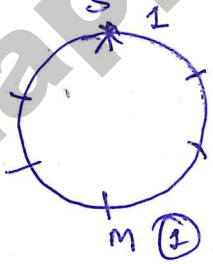
→ Source-down → orphan packet.
→ corrupted packet
} → Monitor bit

* If our source is down then who will remove that packet from the ring.?



These packet are called the orphan packet.

Solution:



→ After sending a packet, the sender went down.
→ The monitor node first time marked that packet as one.
→ If that packet come again to the monitor then monitor will removed that packet from the ring considered as orphan.

Gate-appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

→ Token problems → Captured, Lost or corrupted

* Monitor keeps track of maximum token return time
If token doesn't return in that time then monitor created the new token.

→ Destination → down or busy

↳ Available and copy bits used by the destination if destination is down and busy.

* The destination re-set the monitor bit for negating the monitor effect.

→ Link → down/cut.

→ Monitor → down.

↳ monitor keep sending Active monitor presence at regular Interval to all host [Heart beat msg].

Gate.appliedcourse.com

gatecse@appliedcourse.com

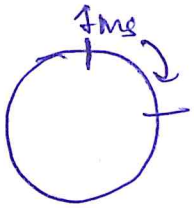
APPLIED COURSE
Ph: +91 844-844-0102

One. Token-holding time = 1ms

B = 16Mbps

Max frame size = ?

Ans.

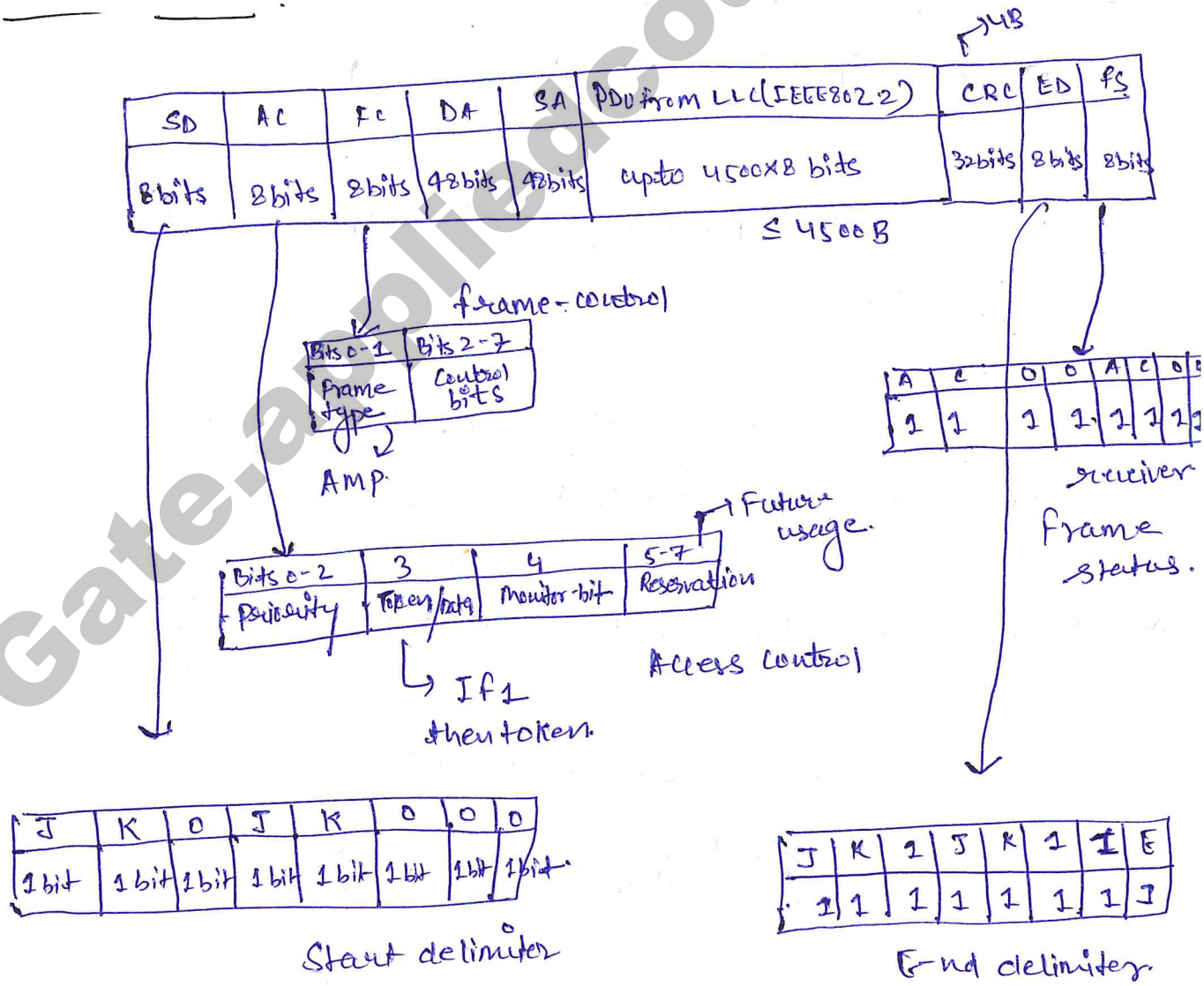


while holding a token how many bit you can transfer.

$1s = 16 \times 10^6$ bits

$1ms = 16 \times 10^6 \times 10^{-3} = 16 \times 10^3$ bits.

Frame Format:



Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

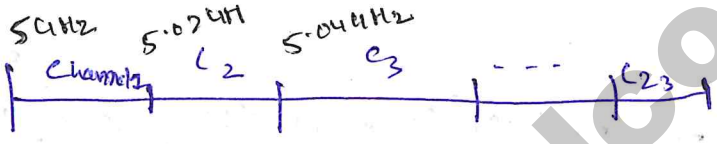
802.11 [WLAN] Wireless LAN.

→ CSMA/CA (ACK, RTS/CTS)

→ Wireless : 2.4GHz, 5GHz.

→ Medium is air [Radio] [EM waves]

5GHz means → 23 non-overlapping half-duplex channels.



$1GHz = 1000MHz$

$20MHz = 0.02GHz$

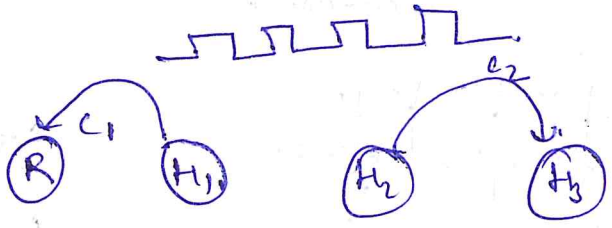
C_1 : 5.502 GHz

C_2 : 5.02 – 5.04 GHz

⋮

* Here we are dividing the 5GHz frequency in 0.02 GHz. Like that 23 channels possible.

* By using this H_1 and H_2 can transfer on different channels



Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que Consider a simple communication system where multiple nodes are connected by a shared broadcast medium (like ethernet or wireless). The nodes in the system use the following carrier-sense the mediums access psotocol. A node that receives a packet to transmit will carrier sense the medium for 5 units of time. If the node does not detect any other transmission in this duration, its start Transmiting the packet in the next time unit. If the node detects another transmission, it waits until this other transmission finishes, and then begins to carrier sense for 5 time units again. Once they start to transmit, nodes do not perform any collision detection and continue transmission even if collission occurs. All transmissions last for 20 units of time. Assume that the transmission signal travels at the speed of 10 meters per unit time in the medium.

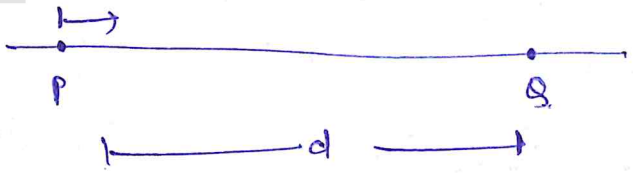
Assume that the system has two nodes P and Q, located at a distance d meters from each other. P starts transmitting a packet a time $t=0$ after sucessfully Completing its carrier-sense phase. Node Q has a packet to transmit at time $t=0$ and begins to carrier sense the medium.

The maximum distance d (in meters, rounded to the closest integer) that allows Q to sucessfully avoid a Collision between its proposed transmission and P's on going transmission is ?

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Sol.



Carrier sense = 5 units

T_f = 20 sec

V = 10 m/s

The time taken a frame to reach Q is $= \frac{d}{10}$

$\Rightarrow$ To avoid collision our frame from P should reach to Q.

$\Rightarrow \frac{d}{10} \leq 5$

$d \leq 50 \Rightarrow \max d = 50$.

Que. In an Ethernet local area network which one of the following statements are true ?

(A) A station stops to sense the channel once it starts transmitting a frame.

(B) The purpose for the jamming signal is to pad the frames that are smaller than the minimum frame size.

(C) A station continues to transmit the packet even after the collision is detected.

(D) The exponential backoff mechanism reduces the probability of collision on retransmissions.

gatecse@appliedcourse.com
Gate-appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

(A) → false because it also has to detect the collisions.

(B) → Jamm signal is used to inform the hosts but not for padding.

(C) → Once the collision is detected station stops transmitting.

(D) → True, Yes exponential backoff algorithm used for retransmission which reduces the probability of collision.

Qu: For the IEEE 802.11 MAC protocol for wireless communication, which of the following statements is/are TRUE?

I. At least three non-overlapping channels are available for transmission.

II The RTS-CTS mechanism used for collision detection.

III Unicast frames are Acked.

Sol: I. for 2.4GHz we have = 3 channels
for 5GHz we have = 5 channels } → True.

II. There is no collision detection we have collision avoidance. } → false.

III. True, Unicast H_i —— H_j
One node to one node = Unicast.

Ans → I and III only.

Gate.appliedcourse.com
gatecse@appliedcourse.com

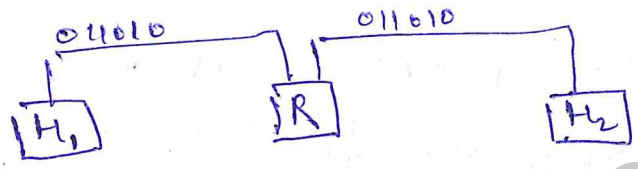
APPLIED COURSE
Ph: +91 844-844-0102

Network devices:

Repeaters

→ Physical-layer device.

→ 2 port.



Copies data to original-signal-strength.

→ Repeaters are used to re-gain the strength of the signal.

→ If the signal is weak and is not reaching to other host. We use repeater to place it in-between two hosts.

→ It only works on encoding of data and repeats the signal.

Gateappliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

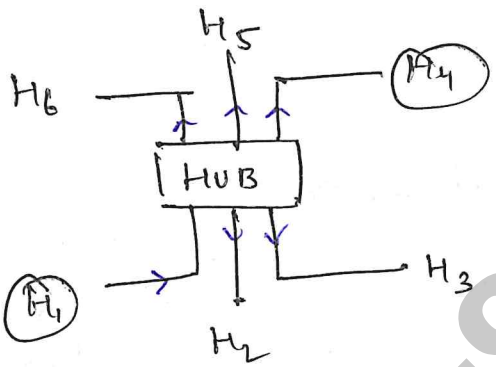
HUB :- → physical layer device

→ Multiport - repeater.

→ no-intelligence.

→ Cannot filter data

→ Cannot find best paths.



It transfer the data in all directions, not an intelligent device.

* It just copies the data from one port and repeat the data to all other ports by maintaining the original strength of signal.

Active: Own power supply. Repeater + wiring - center.

Passive: Cannot repeat, just relay signals.

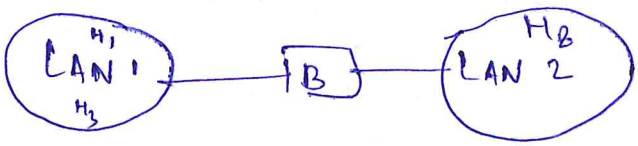
Bridge:

→ DLL - device → frame MAC → Ethernet, Token ring, WLAN

→ Connect 2 - LANS

→ filter based on MAC

→ Transparent vs Source - routing bridges



* It uses mac address to filter. If H_1 send data to H_2. Bridge forward to LAN 2.

gatecse@appliedcourse.com
Gate.appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Source routing bridges exactly follows the path $H_1 - H_6 - \ldots - B \rightarrow H_7 - H_8$ suggested by the source.

Switch:

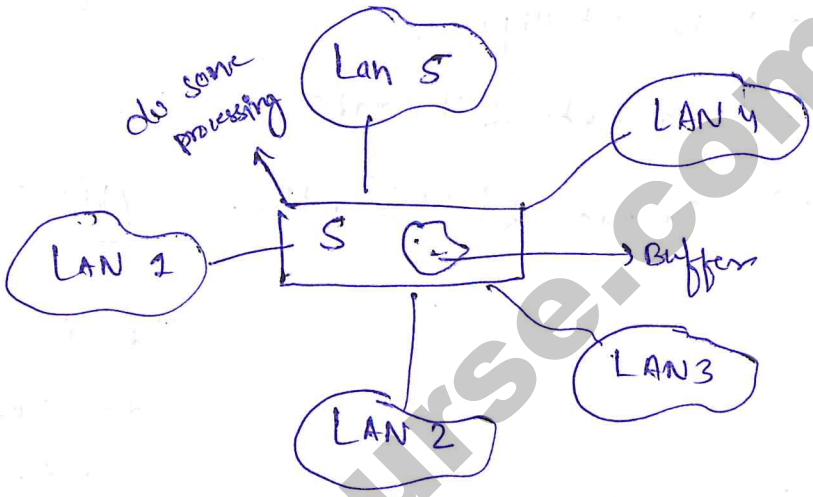
→ Multiport-bridge

→ Buffers

→ DLL device

→ error check before forwarding

→ forwards to the correct port



* Switch also uses MAC address for forwarding. It has buffer and some processing unit which checks whether sending frame is correct or not.

Routers:-

→ routes packets based on IP-addresses.

→ Network layer device.

→ routing-tables.

→ connect LANs and WANs.

Gate.appliedcourse.com
gatecse@appliedcourse.com

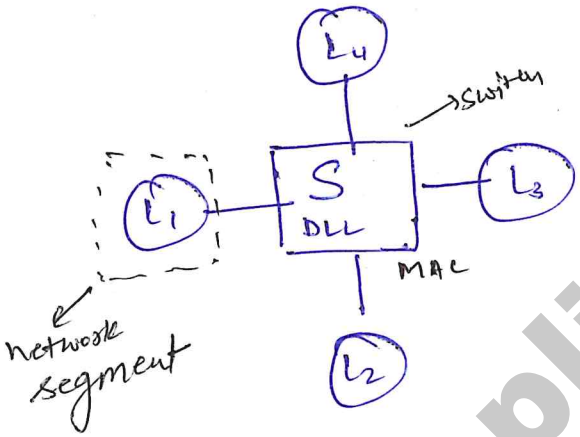
APPLIED COURSE
Ph: +91 844-844-0102

Brouter:

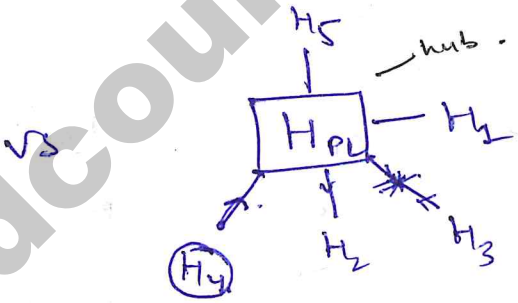
→ DLL and Network - Layer device.

* It performs task of both DLL and network layer.
* So, it can perform the task of both.

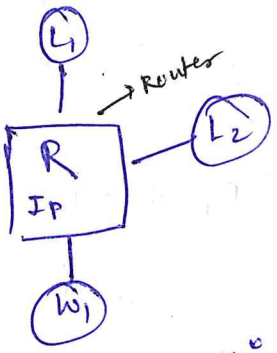
Most Popular devices: Switches and Routers



vs



vs



Network segment:- Network segment is collection of hosts

We can consider one LAN as one segment.

	Switch	Hub (not a smart device.)	Router.
Collision domain -	Seperator	Can not break	Seperator
Broadcast domain - (NW L IP)	Can not break.	Cannot break.	Seperator.

We want to broadcast in a LAN.

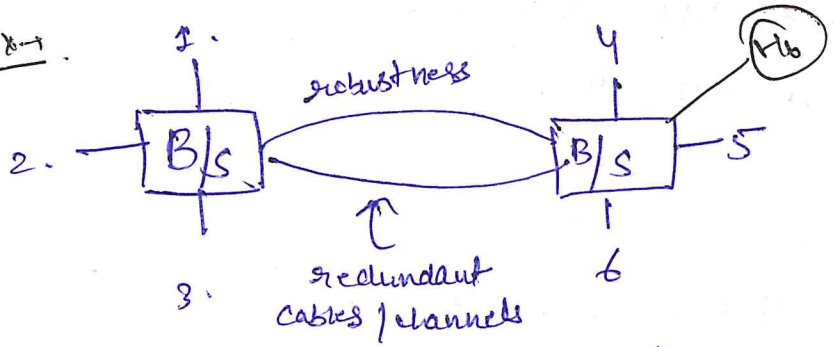
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Spanning Tree Protocol (STP)

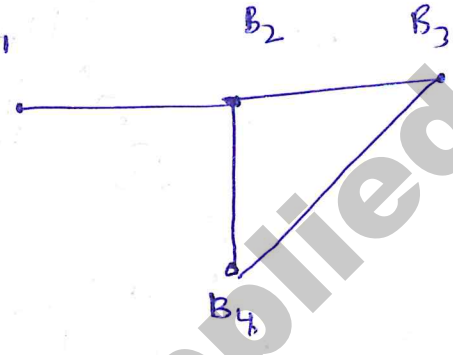
* We learn spanning tree in graph and Algorithms.

Ex-1.



→ we are using two cables for robustness / reliability.

Ex-1. 2

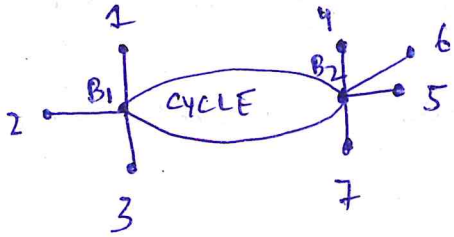


for $B_1 - B_4$ ⇒ $B_1 - B_2 - B_3 - B_4$ or $B_1 - B_2 - B_4$

* If one path goes bad still we are able to transmit via other path.

→ Unknown destination ⇒ flood ⇒ ∞ loops.
↳ If switch doesn't know about any host. It will flood the packet.

→ Spanning tree ⇒



→ You can encounter ∞ loops because of cycle.

Gate-appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

* Spanning tree it covers all the vertices without loops.

Distributed ST-algo:—

→ root node : Smallest MAC [Smallest MAC address will be root node

→ Configuration frames

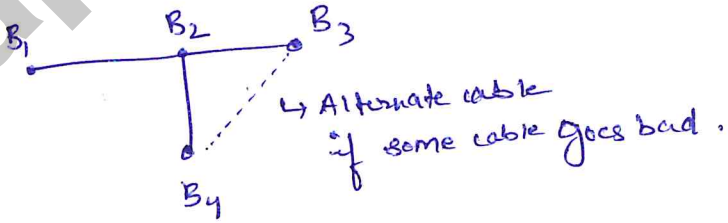
→ Shortest path from root

hops prop time.

* Shortest path from root can be determined on the basis of hops and prop time.

→ IEEE 802.1D → protocol will give you lots of details about how ST-algo / format etc works.

final spanning tree for Ex-2 is



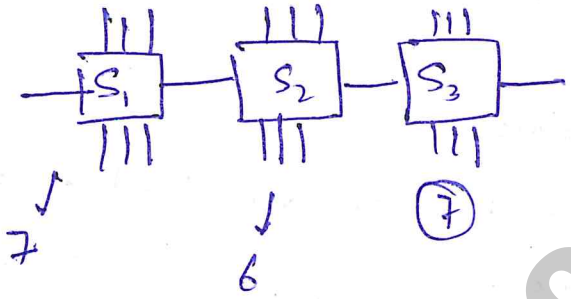
→ Radia Perlman CSE Scientist developed this algorithm.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que: Consider that 15 machines need to be connected in a LAN using 8-port Ethernet switches. Assume that these switches do not have any seperate uplink ports. The minimum number of switches needed is?

Sol: One switch has 8 connections.



Maximum we can connect = 20 using 3 switch.

For 15 we need minimum 3 switch.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Network layer :— (Internet protocol)

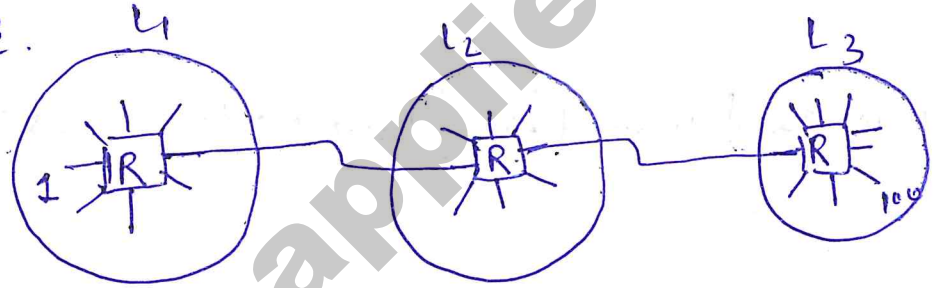
1. IP- address, Subnetting and Supernetting
2. IPV4 and IPV6
3. Routing algorithms.

IP Addressing (IPV4)

→ 32 bit logical address assigned to computer.

Q. Why not use MAC-addr?

Ans.



There are billion of hosts in the network. Each host has unique MAC address.

There is no particular series of MAC address. Every company follows different rule.

If H_1 wants to send the packet to host 100. The router doesn't know any net-id or subnet-id. It is very difficult for router to communicate. So, if router floods the packet to every link this will increase lot of congestion.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
PH: +91 844-844-0102

We don't have hierarchical structure in MAC address.

Like postal address: State
↓
City
↓
Area → Street → house no.

Classfull Addressing

IP address = 32 bit. So, total = 2^{32} addresses possible

(A) | 0 | Network (7) | Host (24) | 1.0.0.0 to 127.255.255.255

(B) | 10 | Network (8+8) | Host (16) | 128.0.0.0 to 191.255.255.255

(C) | 110 | Network (5+16) | Host (8) | 192.0.0.0 to 223.255.255.255

(D) | 1110 | Multicast address | 224.0.0.0 to 239.255.255.255

(E) | 1111 | Reserved for future use. | 240.0.0.0 to 255.255.255.255

* In class A first bit is always zero, next 7 are net bits and 24 are host bits

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

* In Ip address we have four octets.

Range → 0-255 . 0-255 . 0-255 . 0-255
first octet | Second octet | Third octet | Fourth octet

→ In class A the range of first octet is
  * 1 - 126
  * 127 is is reserved as loop back address.

→ In class B 10 is the starting bits always.
  In class B net bits (6+8) = 14 and host bits are 16

→ In class C 110 is the starting bits always
  In class C 21 bits as net bits and 8 bits are host bits.

→ In class D 1110 is the starting bits. The class D addresses are used for multicasting.

→ In class E 1111 is the starting bits. The class E addresses are reserved for future use.

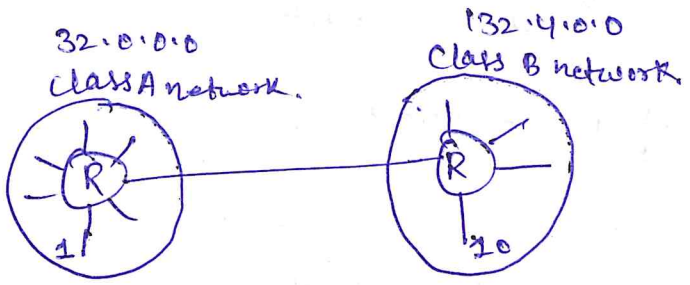
Ranges:

Class	First octet
A	1-127
B	128-191
C	192-223
D	224-239
E	240-255

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

UNICASTING :-



32.1.2.3
Class A address

132.4.5.6
Class B address

→ For getting the Ip address of the network, put all host bits at zero.

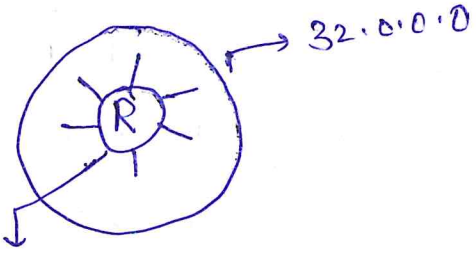
Host address → 32.1.2.3 [Class A address]

So, Network address → 32.0.0.0
(host bits)

→ In Unicasting we are transfering from single host to single host.

Broadcasting :-

Limited :-



SA : 32.1.2.3

DA : 255.255.255.255

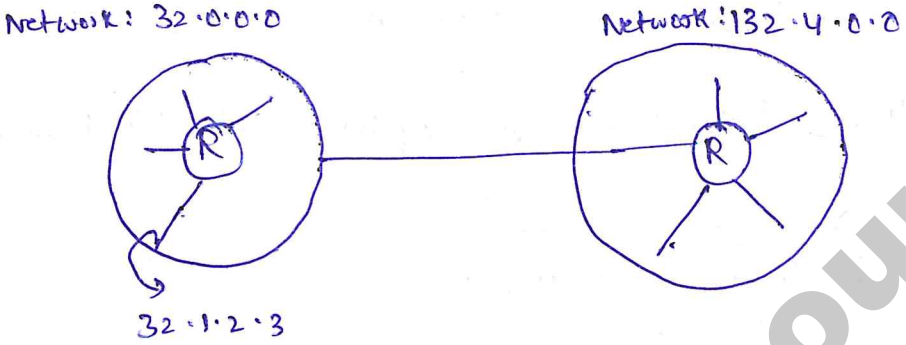
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

→ Limited broadcast is used to send the packet from single host to all the hosts within a network.

Here in destination address put all one's.

Directed broadcast :-



→ Directed broadcast is used to broadcast the packet in the different network.

→ We have to assign all host bit's as one's in the network address of destination network.

SA: → 32.1.2.3

DA: → 132.4.255.255

Host bits all one's.

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Concept:- No. of hosts in a network.

Class A : 1.0.0.0 to 127.255.255.255 [Range]

* In class A eg: 32.0.0.0 [network address]
  → we have 24 host bits in class A
  → So, $2^{24} - (2)$ [Total number of host address possible]

** We are subtracting 2 because:
  → One address is waste in network address
  32.0.0.0
  → Another address is waste in broadcast address
  32.255.255.255

Class B 128.0.0.0 to 191.255.255.255 [Range]

e.g: 132.1.0.0 → $2^{16} - 2$.

→ we have 16 bits for host address
→ So, total number of address is $2^{16} - 2$ [host addr]

Class c : 192.0.0.0 to 223.255.255.255

e.g. 192.1.2.0 → $2^8 - 2 = 254$
(2^8 ← 8 host bits.)

gatecse@appliedcourse.com
Gate.appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Subnetting :-

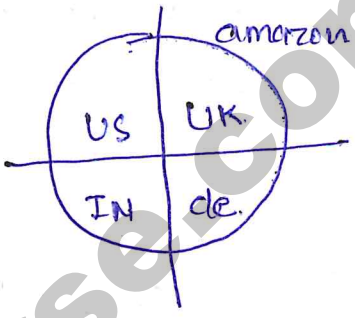
Wire-shark : IP → 52.94.232.33 (Class A) [Amazon-server]

DNS

↓

New-IP: 52.0.0.0 ← for Net addr put host bits zero.

DBC IP: 52.255.255.255

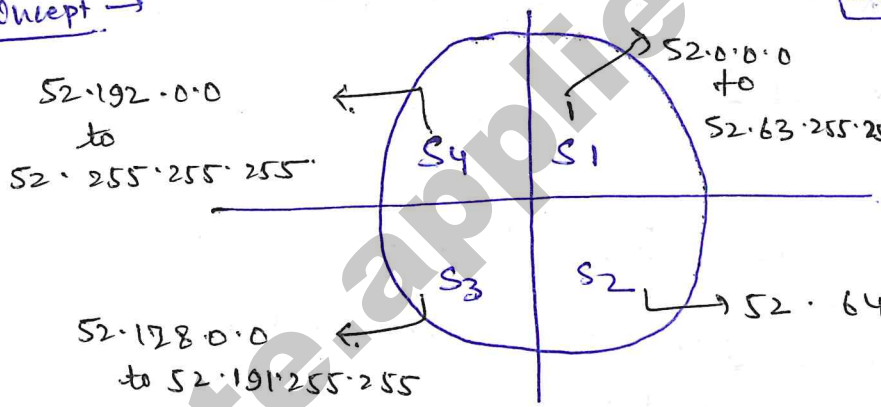


Max No. of hosts = $2^{24} - 2 \approx$ 16 Million.

* For legal and security reasons it's better to break a big network into sub-networks.

Concept →

52.0.0.0 [Network addr]
↳ we want to create four subnets.



S2 → 52.64.0.0 to 52.127.255.255

* In Subnetting we borrow some bits from hosts to create subnets.

52.① ② ③ ④ ⑤ ⑥ ⑦ ⑧ . 0-255 . 0-255

0 0	→ S_1	→ 52.0.0.0 to	52.63.255.255
0 1	→ S_2	→ 52.64.0.0 to	52.127.255.255
1 0	→ S_3	→ 52.128.0.0 to	52.191.255.255
1 1	→ S_4	→ 52.192.0.0 to	52.255.255.255

52.192.0.0 ↓ Subnet id's

52.255.255.255 ↓ DBA of Subnet id's

Gate.appliedcourse.com
gatecse@appliedcourse.com

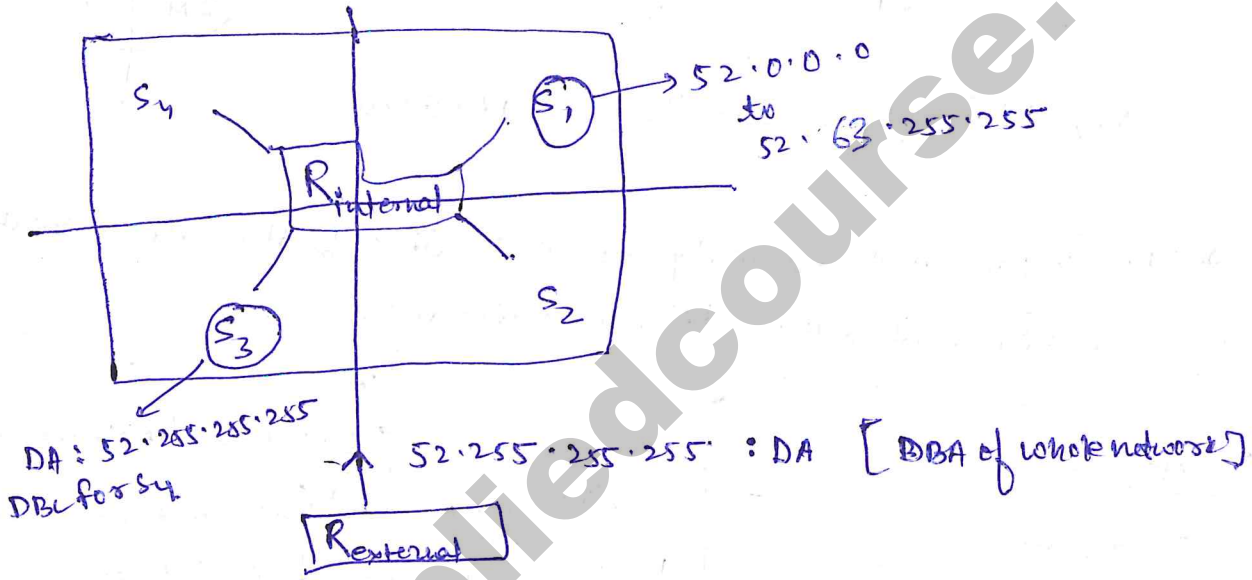
APPLIED COURSE
Ph: +91 844-844-0102

* No. of hosts possible in each subnet is again

* $2^{\text{host bits}} - 2$ ⇒ In last Ex→ $2^{22} - 2$ for each subnet.

Que: 52.255.255.255 ⟶ Direct broadcast of NW or S_4

52.0.0.0 ⟶ NW-IP of NW or S_1



* If a packet coming from internal network.

52.255.255.255 then the packet is treated as broadcast address of S_4

* If a packet is coming from outside network then it is treated as broadcast address for whole network.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Subnet mask : 32-bit

In the subnet mask all the network and subnet bits are 1, host bits are zero.

Ex-1 255.192.0.0 = /10 → Another representation of subnet mask.

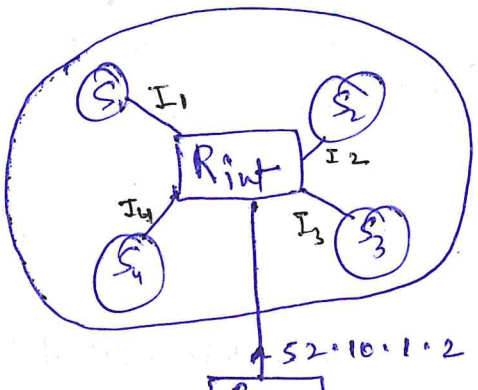
8 | 2 | 000000.0.0
net | Subnet

* Subnet mask is calculated at the time of subnetting itself.

Consider previous figure and Ex:-

Rint: ① [Subnet mask : 255.192.0.0]

② if:
- 52.0 – 52.63 → S_1 (I_1)
- 52.64 – 52.127 → S_2 (I_2)
- 52.128 – 52.191 → S_3 (I_3)
- 52.192 – 52.255 → S_4 (I_4)



If Rint receives the packet with these IP. It will forward to corresponding interface.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

③ else, if the ip dresnot belong this range then use mask 0.0.0.0 and send to R_{ext}

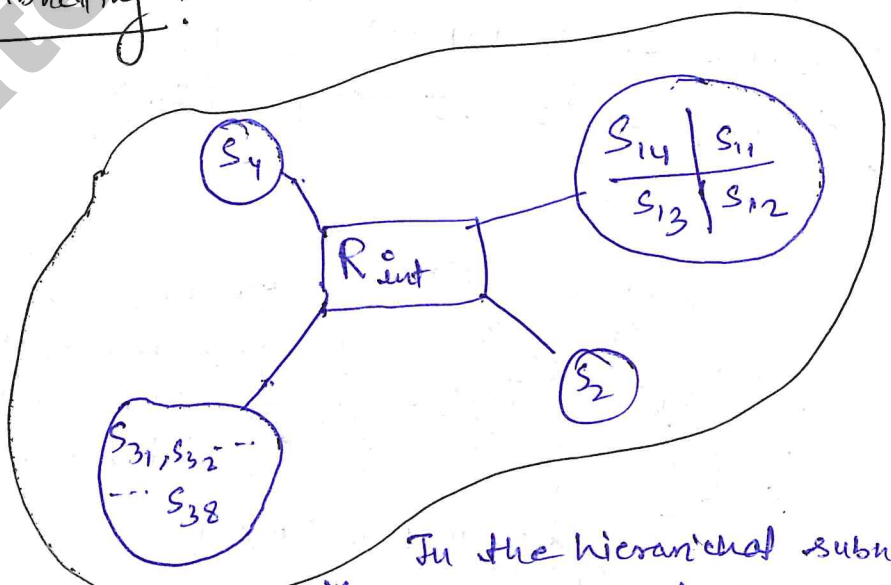
Ex→ If R_{ext} send the packet with IP 52.10.1.2, then R_{int} will perform masking.

Performing logical AND with subnet mask no. and host address will give you subnet id.

52 . 0000 1010 . 1 . 2.
255 . 11 000000 . 0 . 0
AND 52 . 0 . 0 . 0

* By getting the subnet id R_{int} will forward to the corresponding subnetwork.

Hierarchical - Subnetting :

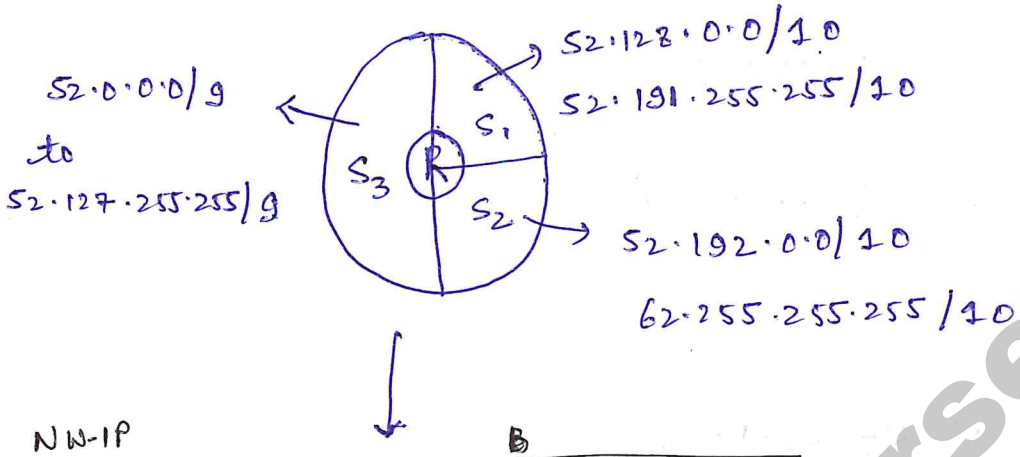


* In the hierarchical subnetting subnets can be further created in subnets.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Subnetting : different Sized - Si's



NW-IP

52.0.0.0/8 to 52.255.255.255/8

/8 → Subnet mask of whole network.

255.0.0.0

Dividing network id [we want to give half of the address to S_2.

Net id → 52.0.0.0

52.0 ——————.0-255.0-255

0 → S_3 [Half of the address]

10 → S_1 [Quarter of the address]

11 → S_2 [Quarter of the address]

So, S_3 ⇒ 52.0.0.0/9 to 52.127.255.255/9

↳ mask no. is 9 because we are using 8 net bits and 1 Subnet bit

S_1 = 52.128.0.0/10 to 52.191.255.255/10

↳ mask no. is 10 because we are using 8 net bits 2 subnet bits.

S_3 = 52.192.0.0/10 to 52.255.255.255/10

↳ mask no. is 10 because we are using 8 net bits and 2 Subnet bits.

gatecse@appliedcourse.com
Gate.appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

R

	Mask	Subnet id	Interface / Subnetwork.
(1)	/9	52.0.0.0	S_3
(2)	/10	52.128.0.0	S_1
(3)	/10	52.191.0.0	S_2.

E.g. D.A. → (a) 52.62.1.2.

↓

Mask with /9 [means take AND with mask and Address]

I get 52.0.0.0 ⇒ S_3 ✓

(b) 52.161.1.2

↓

Mask with first entry /9 ✗ does not get S_3

mask with second entry /10 ⇒ S_1

↳ 52.128.0.0 ✓

(c) 52.200.1.2.

↓

Mask with first entry /9 ✗ doesnot get S_3

Mask with second entry /10 ✗ does not get S_1

Mask with third entry /10 ✓ ⇒ S_2.

This is how internal router do masking.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

[CIDR] Classless - Inter Domain Routing (1993 - IETF)

* The task force created in 1993 started getting problems in classfull addressing.

* In 1993 people started using classless.

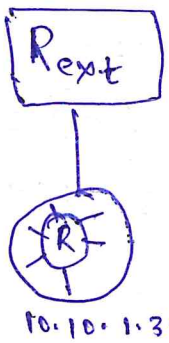
* Assign any Block of IP addresses to any ISP/company/inst
  ↳ IANA

* IANA assigns consecutive Ip addresses upto the number you want. Let's we want 2^{16} addr.

  Eg $a.b.c.d \pm 2^{16}$
  - $a.b.c.d$ → first addr
  - 2^{16} → consecutive addr

* Let's take an Ex: we want 32 IP address for company.

  IANA: → Assigned a block.
  - $10.10.1.32/27$ → This is called block address
  - $10.10.1.63/27$ → This is called BC-IP



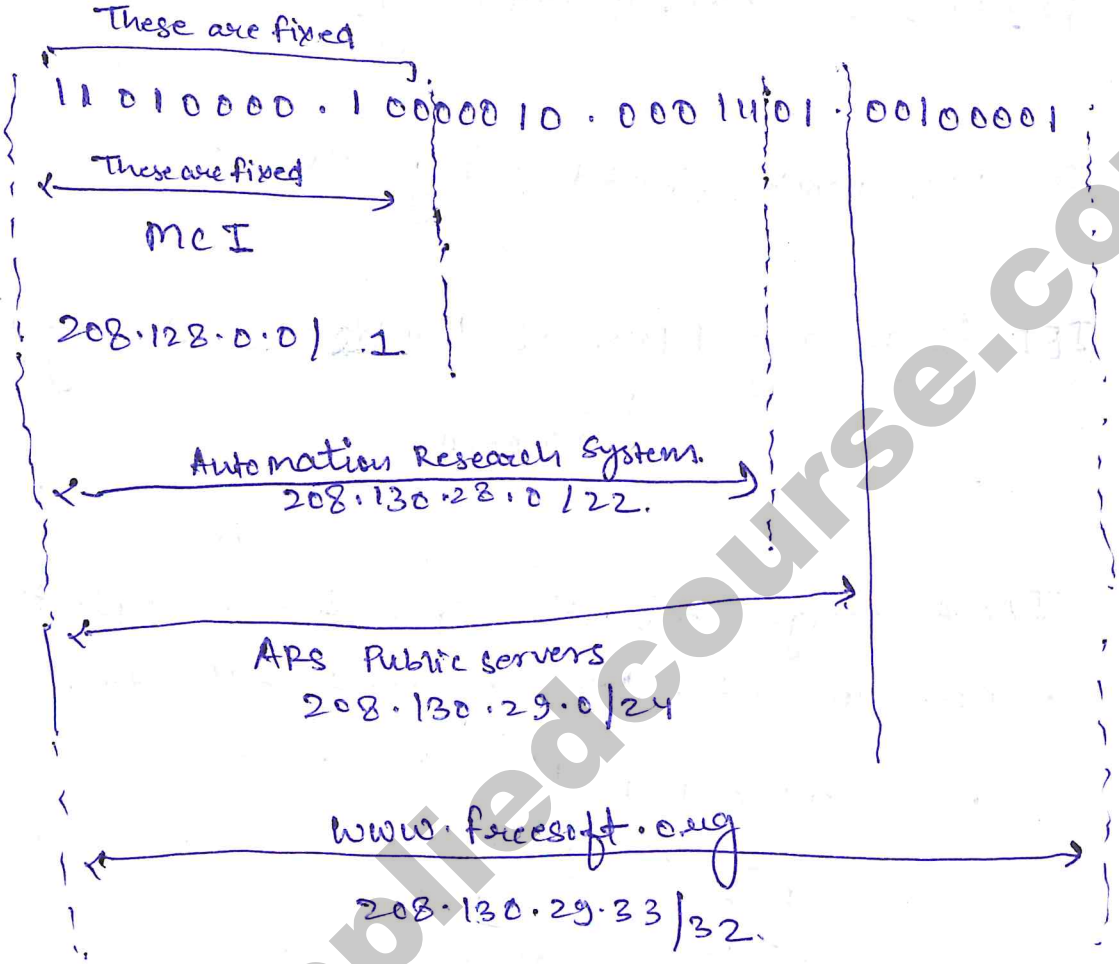
* Router ext will mask the host address
  ∴ If we get the 10.10.1.32
  It will forward to this network.
  OR
  if it does not get 10.10.1.32 and get suppose 10.10.1.90 then Rext will discard.

Gate-appliedcourse.com
gatecse@appliedcourse.com

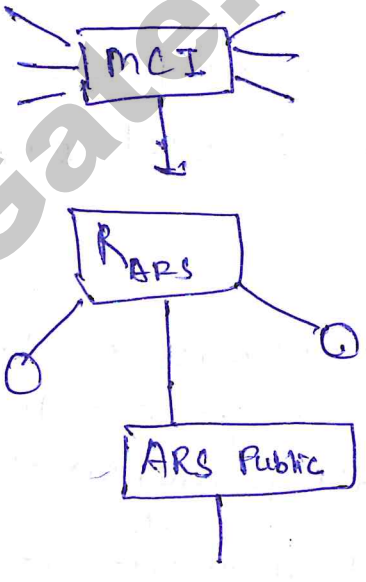
APPLIED COURSE
Ph: +91 844-844-0102

late 1990's

IANA Gave 208.130.29.33



It is a hierarchical subnetting.



IANA → MCI → ARS → PS →
2 mill 2^{10} 2^{8}

IANA assigns to MCI
MCI assigns to ARS some addresses
ARS assigns to PS some addresses.

freesoft.org → only one address assign because /32 is mask.

gatecse@appliedcourse.com
Gate.appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

a.b.c.d /32 → 2^0 → only one host we can assign

a.b.c.d /31 → 2^1 → Two addr possible

a.b.c.d /27 → 2^5 → 32 addr possible

Problems:

Que: Consider three machines M, N and P with IP addresses 100.10.5.2, 100.10.5.5 and 100.10.5.6 respectively. The subnet mask is set to 255.255.255.252 for all three machines. which one of the following is true?

(A) M, N and P all belong to the same subnet

(B) only N and P belong to the same subnet.

(C) M, N and P belong to three different subnet.

(D) only M and N belong to the same subnet.

Ans: 255.255.255.11111100 = /30

For solving this question we have to apply AND between subnet mask and Ip address to get the subnet Id's.

M ⇒ 100.10.5.00000010
255.255.255.11111100
100.10.5.0

N ⇒ 100.10.5.5
100.10.5.00000101
255.255.255.11111100
100.10.5.4

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

P => 100.10.5.00000120
255.255.255.11111100

Subnetid => 100.10.5.4

=> Therefore, N and P belong to the same subnet.

Que: Consider the following routing table at an IP router. For each IP address in Group-I identify the correct choice of the next hop from the Group-II using the entries from the routing table above.

List - I

A. 128.96.171.92.
B. 128.96.167.151
C. 128.96.163.121
D. 128.96.165.121.

List - II

1. Interface 0
2. Interface 1
3. R_2.
4. R_3
5. R_4.

Network No.	Netmask	Next hop
128.96.170.0	255.255.254.0	Interface 0
128.96.168.0	255.255.254.0	Interface 1
128.96.166.0	255.255.254.0	R_2
128.96.164.0	255.255.254.0	R_3
0.0.0.0	Default	R_4

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Codes:

	A	B	C	D
(a)	1	3	5	4
(b)	1	4	2	5
(c)	2	3	4	5
(d)	2	3	5	4

Ans: for each Ip address in List-1 we have to find the correct choice of next hop.

A ⇒ We will perform AND between

128.96.171.92
255.255.254.0

128.96.170.0

So, A will go to interface 0.

c and d options can not be the answer.

B ⇒ 128.96.167.151
255.255.254.0

128.96.166.0

B will go to R_2.

Hence answer is a.

167 ⇒ xxxxxxx 1
254 ⇒ 1111111 0
---
xxxxxxx 0
⇓
166

Short trick.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que: In the network 200.10.11.144/27, the fourth octet (in decimal) of the last IP address of the network which can be assigned to host is —

(a) 158
(b) 255
(c) 222
(d) 223

Ans: 32 - 27 = 5 host bits.

200.10.11.144

last octet =>

=> 1 0 0 1 0 0 0 0 = 144

network

So, Max 1 0 0 1 1 1 1 1 → Largest host

So, 158 is the last octet.

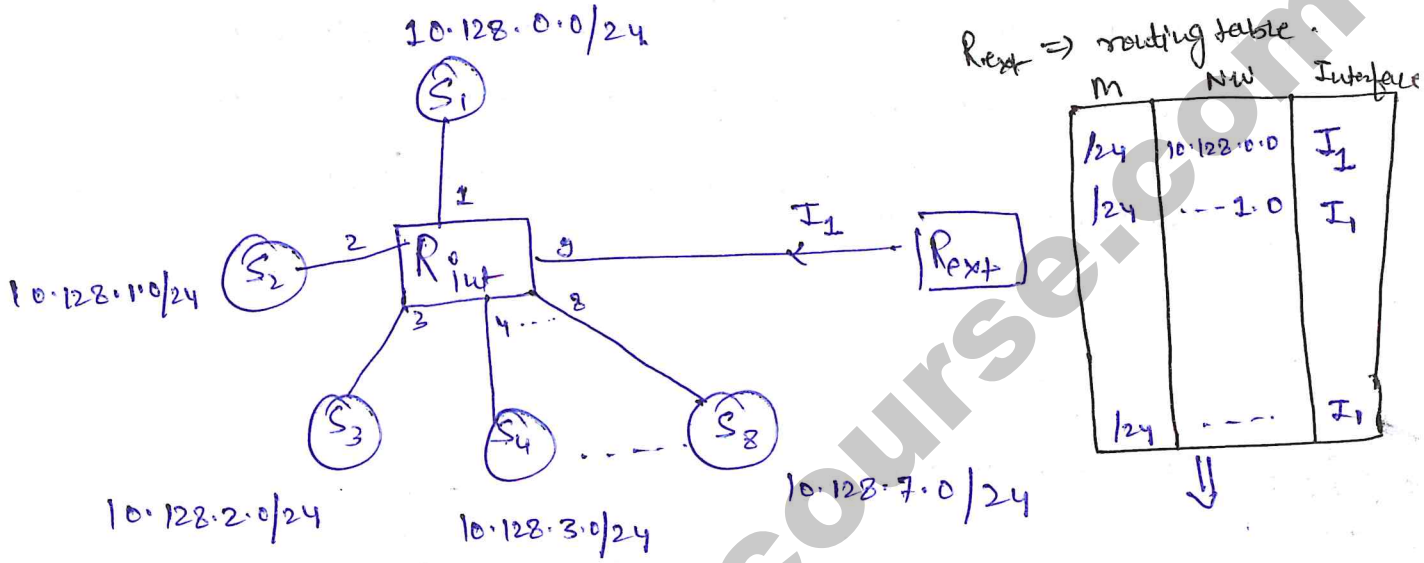
Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Supernetting:-

In supernetting we combine two networks logically.



Rext will see the corresponding mask no. and network address. Forward it to interface.

Rint table:

M	NW	Interface
/24	10.128.0.0	1
/24	10.128.1.0	2
⋮		⋮ 8
/24		
/0	Default	9

* The routing table of Rext is becoming too large because of the subnets are more. The size of Rext routing table is not sufficient to handle this big data. If n etries their we need O(n) time to decide which interface we need to send.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

* In Supernetting, we are logically combining the subnetworks with the objective of reducing the size of external routing table.

Example -

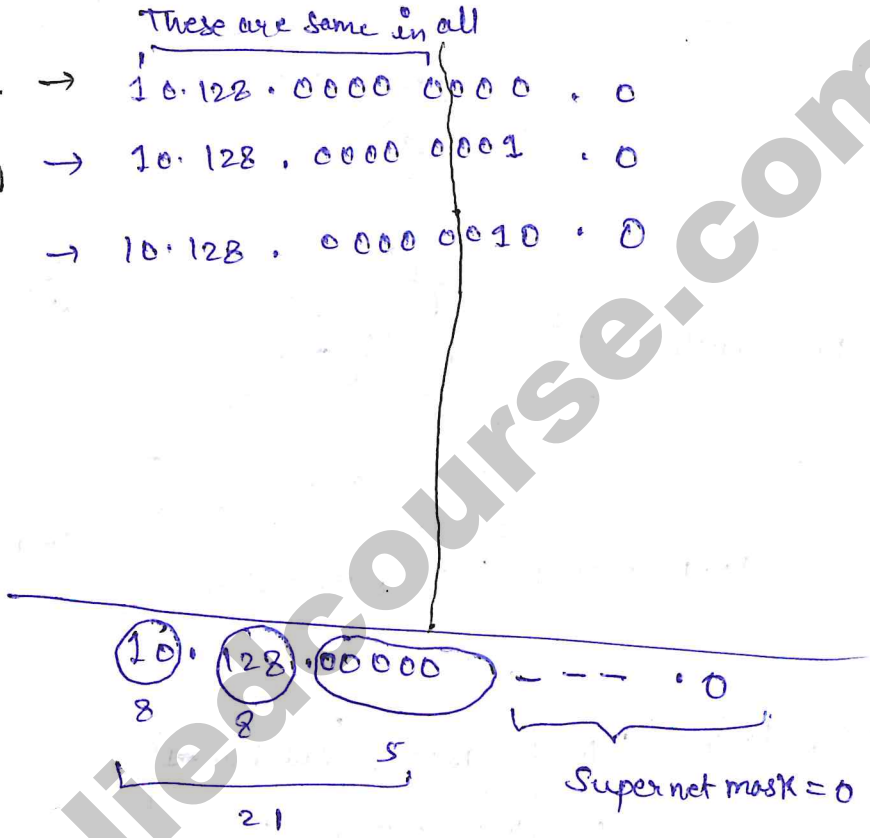
S_1 : 10.128.0.0/24. → 10.128.0000 0000.0

S_2 : 10.128.1.0/24 → 10.128.0000 0001.0

S_3 : 10.128.1.0/24 → 10.128.0000 0010.0

⋮

S_8 : 10.128.7.0/24



Here we are changing our mask number from 24 to 21 [Because upto 21 all bits are same] for all subnets.

Now, In Next table.

M	NW	Interface
/24	--	I_1
/24	--	I_1
⋮		
/24	--	I_1

Previous table

→

NW IP	mask	Interface
10.128.0.0	/21	I_1

We are replacing these 8 entries with single entry.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

E.g: Rext get 10.128.7.6 as the destination address.

= Rext will mask with 21.

10.128.00000111.00000 110
255.255.11111000.00000000

10.128.0.0

Hence, Rext will send this packet to Interface 1.

E.g DA: 10.128.3.12 ⇒ Rext get this packet

= 10.128.00000011.0 0001100
255.255.11111000.00000000

10.128.0.0 ⇒ Packet sent to Interface 1.

Example – 2

First 4 bits are same in all so keep them same.

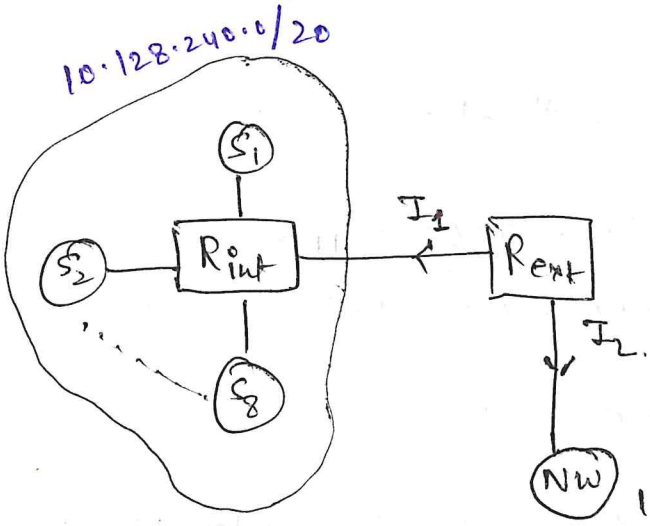
S_1	10.128.247.0	10.128.11110 111 .0
S_2	10.128.248.0	10.128.11111000.0
S_3	10.128.249.0	10.128.1111100 1 .0
⋮		⋮
S_8	10.128.254.0	10.128.1111111.0 .0

10.128.240.0/20 ⇐ 10.128.1111_ _ _ _ .0

Supernet mask = /20 ⇒ 1

gatecse@appliedcourse.com
Gate.appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102



Routing Table

10.128.240.0/20	, I_1
10.128.241.0/8	, I_2

Eg: DA: 10.128.241.3 → 10.128.1111 0000.0 → I_1 (INCORRECT)

When mask with /20

* It should have been sent through I_2 .. this would be more appropiate. Just I_1 entry is above than I_2. It has sent to I_1.

This is incorrect supernetting.

Necessary condition to perform correct supernetting.

S_1 : 10.128.247.0/24
S_2 : 10.128.248.0/24
S_3 : 10.128.249.0/24
⋮
S_8 : 10.128.254.0/24

⇒ we got Supernet mask /21 for this.

The lowest Subnet address ⇒ 10.128.247.0

10.128.1111 0111 ✗
21 0000 ✓

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

→ After 21 bits of mask. everything should be zero in the lowest subnet address.

→ This way you will get the correct supernetting.

Necessary conditions:-

(1) Smallest address divisible by /x that is obtained post supernetting

(2) IPs must be in sequence

(3) $2^1, 2^2, 2^3$ ← Networks combined in powers of 2.

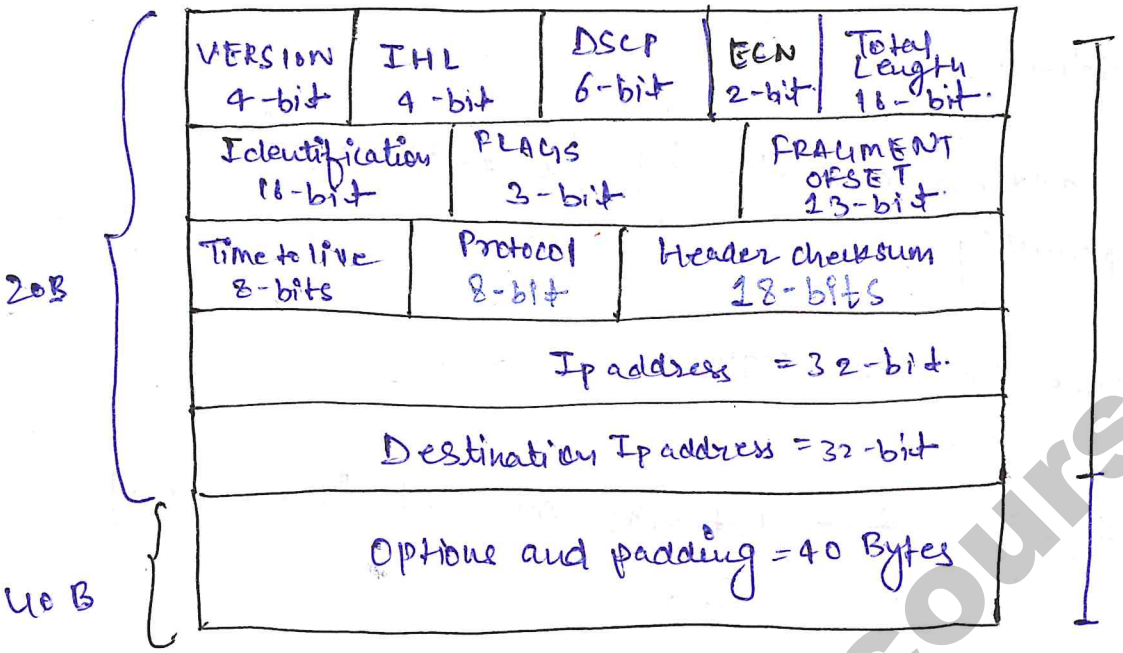
Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

IPV4 : Packet format

Header :



Version → version tells us which Ip version you are using

0100 = IPV4
0110 = IPV6

IHL : Internet header length → It tells what is the length of the header

20B is the mandatory. [Min HL]

Concept → what ever the value in IHL field multiplied by 4 will give you header length.

→ 1111 = 15 × 4 = 60B (IHL)

→ 1010 = 10 × 4 = 40B

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

IHL minimum field = 0100 = 5 × 4 = 20 B

* If your header length → 20 + 31 B = 51 B
(20 ↓ Mandatory)

↳ 51 B is not divisible by 4

→ Add 1 B padding = 52/4 = 13 ⇒ (IHL = 13) ✓

③ DSCP (Differentiated - services code point) - wiki

↳ Types of service { VoIP & Videochat.

Ex→ 101 110 ⇒ Expedited forwarding [Forward as soon as possible]

000 000 ⇒ Best effort

④ ECN (Explicit congestion Notification)

→ often combined with Type of service field

→ To notify that there is congestion.

⑤ Total length (16-bit) → It will give you the size of whole packet.

→ 2^{16} = 64 KB (Max size: header + data)

→ 20 B: min size [Here let suppose we don't have any data.

IP packet

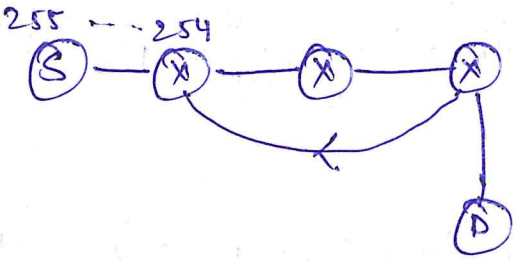
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

(6) Source and Dest Ip : 32-bit each

(7) Time to live : 8-bit field.

→ Count on numbers hops you have.



⇒ If a packet is continue looping will create a lot of congestion.

Max value (8-bit) = 255

→ Max no. of hops = 255 = 11111111

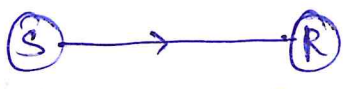
→ In each hop value decrease by 1.

→ If your value is zero your packet will be dropped.

→ changed by the routers in between.

TERM:

DATAGRAM : Packet of an unreliable service.



In un-reliable service we don't get the acknowledgment for the sending packet.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

(8) Protocol →

→ Protocol of the data part (TCP/UDP/...)

→ List of IP-protocols numbers (wiki)

→ ICMP/IGMP/UDP/TCP } → Transport layer protocol.

It tells us what protocol is used in the data field of IP packet.

(9) Header-Checksum:

→ data checksum are used

→ Header checksum itself filled with zeros to compute the checksum } → It is computed by sender

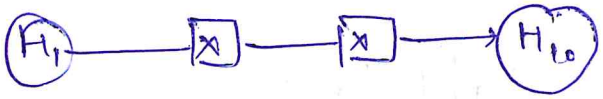
→ Router: TTL changed on every router ⇒ checksum also changed. + other field may change

So, for solution router again re-computes the checksum.

(10) options: (ISP and network managers)

It is used by the ISP providers or network managers.

(a) Route-recording: —



SA = H_1

DA = H_{10} Route recording is used for recording the route.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Like → | R_1 | R_2 |
32 Ip 32 Ip

Options = max 40B.

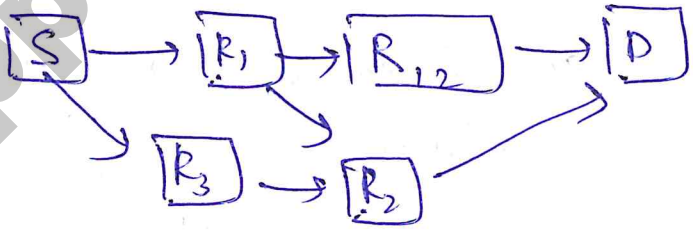
{ 10 Ip address in between route can be stored.

→ But actually we are able to store max 9 Ip addresses because 2B are reserved for future.

So, in $\frac{38B}{4B} = 9$ IP

(2) Source-routing option:

(a) Strict Source routing :-



Means always take the mention path.

| R_1 | R_{12} | D | fixed cannot change

(b) Loose source routing :-

| R_1 | R_2 | D |

R_{12} D → we can also take alternate paths

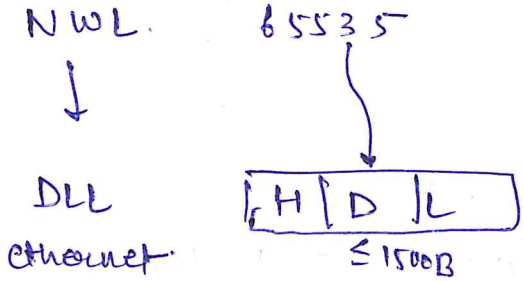
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Fragmentation →

fragmentation means break something up into smaller pieces.

The size of Network layer packet is 65535 Bytes.



The packet is placed in frame.

So, the whole packet we can not transfer directly we have to break the packet.

MTU (maximum transmission unit)

MTU for ethernet is 1500B.

→ Every network has its MTU field.

ID (16-bit) → Every datagram has unique ID which is given in Network layer.

FLAGS (3-bit). First bit always zero not used.

0 Df Mf

Df means do not fragment.

DF = 1 (It denotes it is packet)

DF = 0 (It is a fragment)

Gate.appliedcourse.com
gatecse@appliedcourse.com

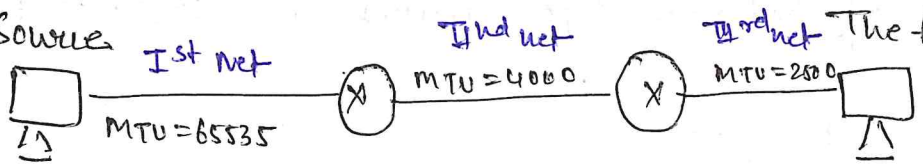
APPLIED COURSE
Ph: +91 844-844-0102

MF (More fragments)

MF = 1. (It is an intermediate fragment)

MF = 0 (It is a last fragment)

Ex →



Original Packet: -

ID	offset	More frag	Pay load
578	0	0	10,000

20B = 10,020 B

for first network we need not to fragment the packet because MTU > Packet size.

R1 —2nd— R2 In 2nd Network MTU is = 4000B

MTU < Packet size.

So, we need to do fragment

* Number of fragments for network 2 = $\frac{10,000}{3980}$ = 2.51 = 3 fragments

R2 — R1

	ID	offset	MF	
Fragment 1	578	0	1	3976

20B

MTU = 2500

F_{11}: 578 | 0 | 1 | 2480

F_{12}: 578 | 310 | 1 | 1496

Fragment - 2	578	497	1	3976

MTU = 2500

F_{21}: 578 | 497 | 1 | 2480

F_{22}: 578 | 807 | 1 | 1496

Fragment - 3	578	994	0	2048

MTU = 2500

F_{31}: 578 | 994 | 0 | 2048

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Fragment 1 offset = 0 because start with first byte.

fragment 2 offset = 497 because start with $\frac{3976}{8}$ = 497th byte

fragment 3 offset = 994 because start with $\frac{3976+3976}{8}$ = 994th byte

** Note → Now question is why we are using 3976 bytes instead of 3980 in starting?

Ans: * Because our payload should be always divisible by 8

3980 → not divisible by 8

3976 → divisible by 8.

*

→ Fragment 1 further divided into fragment 11 and fragment 12

3976 > MTU

2 fragments possible.

Identification number will always same for all fragments.

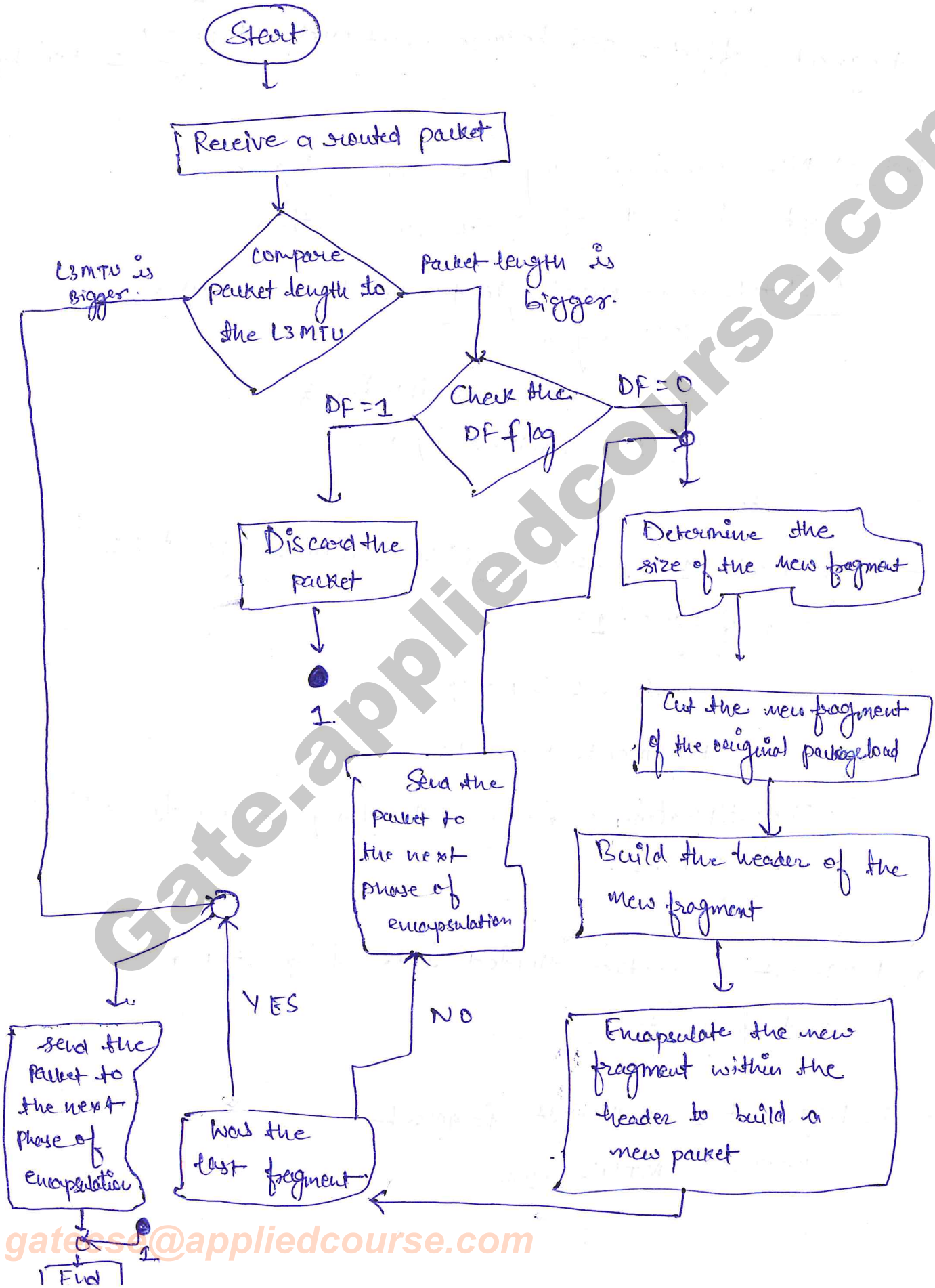
→ Fragment 2 further divided into fragment 21 and fragment 22

→ fragment 3 will not fragment because MTU > 2048

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Fragmentation Algo (IPV4)


Start
Receive a routed packet
Compare packet length to the L3MTU
L3MTU is bigger.
Packet length is bigger.
Check the DF flag
DF = 1
DF = 0
Discard the packet
1
Determine the size of the new fragment
Cut the new fragment of the original payload
Build the header of the new fragment
Encapsulate the new fragment within the header to build a new packet
Was the last fragment
YES
NO
Send the packet to the next phase of encapsulation
Send the packet to the next phase of encapsulation
1
End

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que. Consider an IP packet with a length of 4500 bytes that includes a 20-byte IPv4 header and 40-byte TCP header. The packet is forwarded to an IPV4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0. The fragmentation offset value stored in the third fragment is ____.

600 - 20 = 580 B data.

Ans:

	Offset	MF	Data.
F1:	0	1	576B → It should be divisible by 8
F2:	72 (576/8)	1	576B
F3:	144	1	576B

the fragment should be divisible by 8

The fragment offset for third fragment is 144.

Gateappliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Que The maximum number of IPV4 router address addresses that can be listed in the record route (RR) option field of an IPV4 header is ——.

Ans:- 40 B → optional

2 B → Reserved

38 B left

In $\frac{38\,B}{4\,B}$ = 9 IP addresses possible

Que: An IP datagram of size 1000 bytes arrive at the router. The router has to forward this packet on a link whose MTU (maximum transmission unit) is 100 bytes. Assume that the size of the IP header is 20 bytes. The number of fragments that the IP datagram will be divided into for transmission is: ?

Ans: Data = 80 B Header = 20 B No. of frag = $\frac{980}{80}$ = 12.5

F1 80 B → 80 divisible by 8 no problem.

	offset	
F1	0	80 B
f2	10	80 B
F3	20	80 B
	⋮	

12.5 = 13 fragments ✓.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

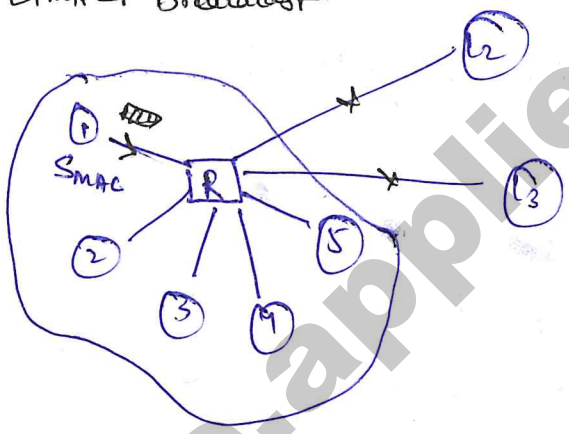
Que: Which of the following fields of an IP header is not modified by a typical IP router?

(a) checksum (b) Source address (c) Time to live (TTL) (d) Length.

Ans → b Checksum → modified
Source address → not modified
TTL → modified
Length → modified

IPV4: Broadcasting

(1) Limited Broadcast.



→ To communicate in the same LAN we use Ethernet protocol

SA: IP_1

DA: 255.255.255.255. → Router after seeing this will not transfer to the other LAN's.

In limited broadcast the destination address contains all one's.

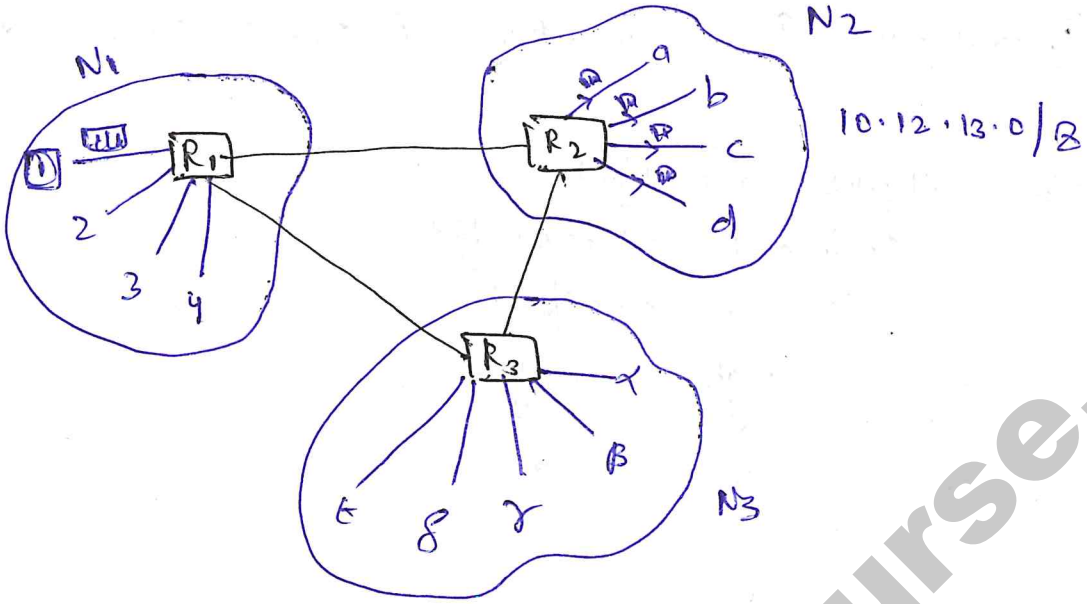
DLL: S_{MAC}

D_{MAC}: all F's] → 12 digit hexadecimal number 48 bit. All F's means broadcasting.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

5) Directed Broadcast : In directed broadcast we are sending a broadcast packet in the other network.



SA: Ip address of host 1 from N1

DA: 10.12.13.255 → DBC - IP for N2.

Packet reached to R_2

R_2 looks the destination address

So, R_2 in DLL sets to all F's

Now, all hosts of N_2 can get the packet

Local host (Loopback) / Localhost.

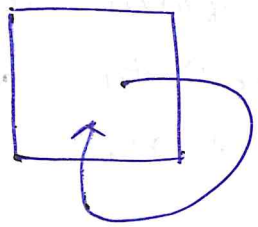
→ 127.0.0.1 [Reserved IP address]

* Using loopback address we can test the connection with our own computer.

* It is a delay of sending a packet to node to itself

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

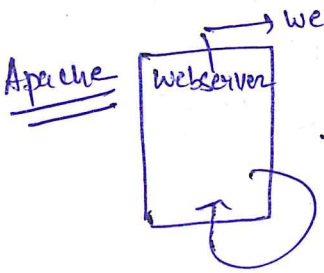


→ Ping (or) http://localhost

→ Debugging | Testing

* It is used to debug or test the network.

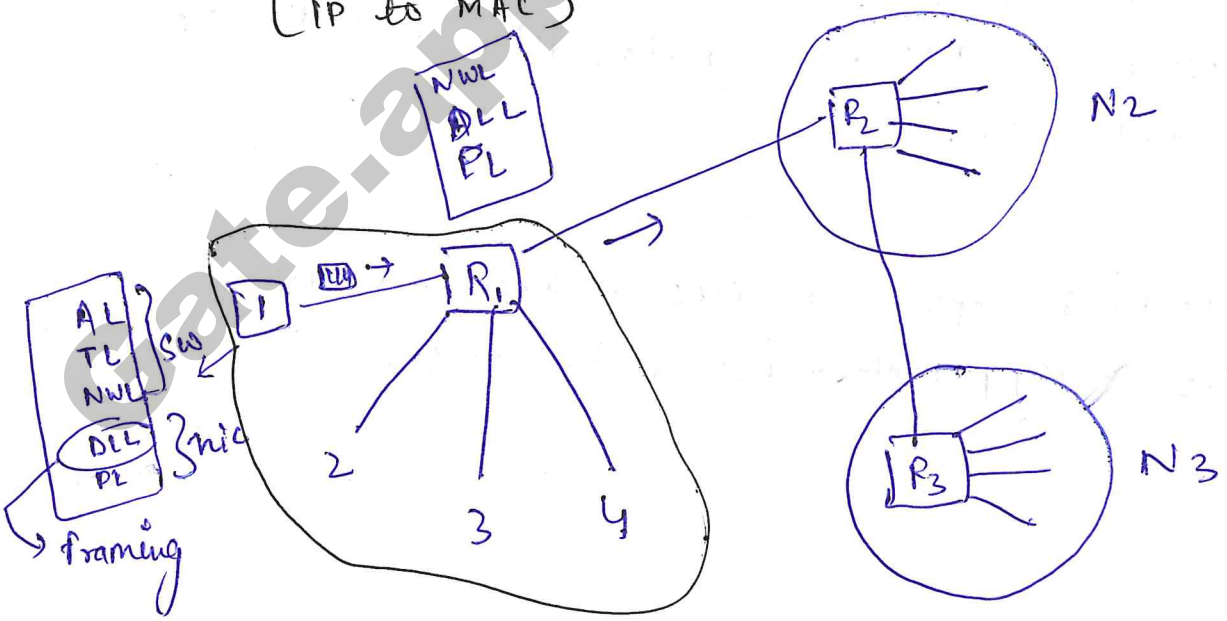
* localhost is also used to test the webserver.



→ It is used to test the server on our own computer.

Address Resolution Protocol (ARP)

(IP to MAC)



→ When you send a packet your host works on several layers before sending the packet.

gatecse@appliedcourse.com
gate.appliedcourse.com

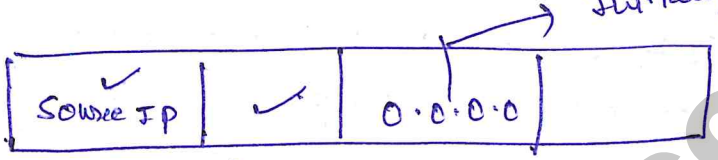
APPLIED COURSE
Ph: +91 844-844-0102

→ Now, when Host 1 sends the packet it sends the packet with Ip address of destination and MAC address of R_1 is unknow to H1,

→ ARP → Address resolution protocol helps us to resolve the MAC address of the destination.

It works on req and reply scheme.

Host 1 wants the mac address of destination router R_1



ARP request packet

This is a broadcast packet

* This request packet will be transfer to all the hosts in the LAN. Whoever has this destination IP will reply.

* So, Router 1 replies with MAC address and updates on the reply packet and send to host 1.

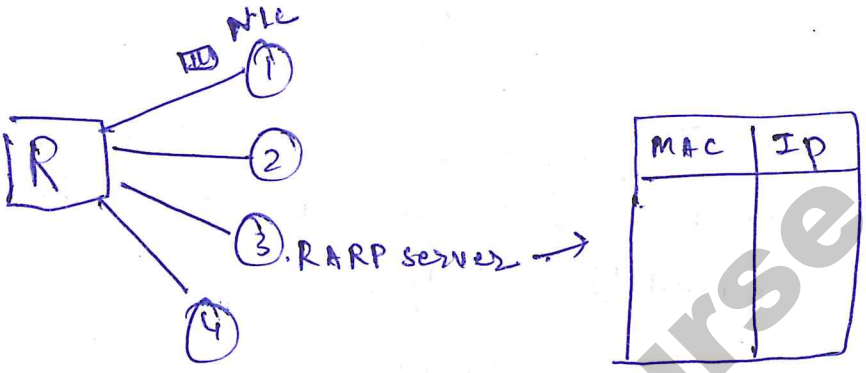
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

RARP: MAC to IP

Reverse Address resolution Protocol

→ MAC fixed
IP : variable



* RARP is used to get the IP address
* Host 1 wants an IP address, so it broadcasts by using all F's in the MAC address in the data link layer.

The RARP server replies with the response if it has the entry of MAC in the table.

If it is a new computer then RARP server creates the entry of the new mac address and sends the new IP address.

Gateappliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

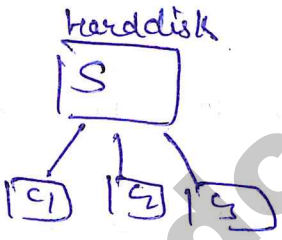
BOOTP (1985) [MAC - IP]

→ Bootstrap protocol.

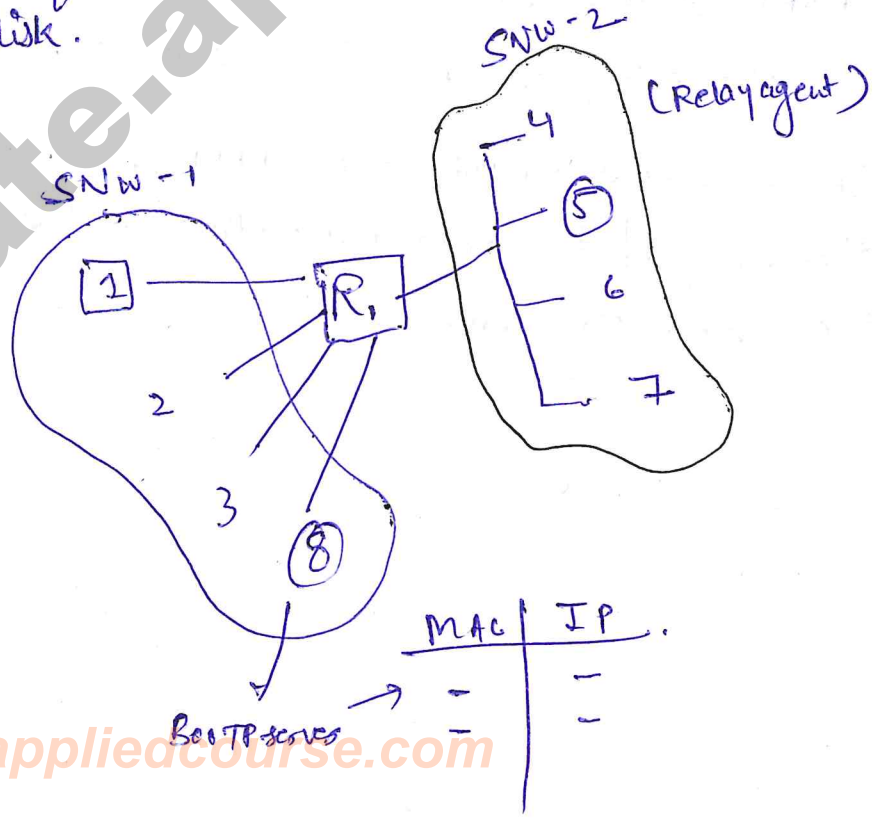
→ Application layer protocol

→ Created for Linux thin clients

Thin clients mean: The systems who have less memory or power. They rely on server for the computational help.



* BOOTP is not the popular protocol now-a-days
* BOOTP protocol are also used for getting the IP address for the thin clients who have no memory or disk.



Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

It is also like RARP request where you the host request for IP by sending a broadcast packet. The BOOTP server will respond with the reply.

* The concept of relaying help us to get only one BOOTP server amongst all subnetworks.

Ex→ In the subnetwork 2 Host 5 wants an IP address. when host 5 send the broadcast packet to all the hosts. The relay agent is the special node which knows the address of BOOTP server.

Relay agent sends the unicast request to BOOTP server and BOOTP server will reply with the IP address afterwards relay agent send the IP to host 5.

* The drawback in RARP/BOOTP is they have static table on the server.

The static table contain the IP address and mac address. The IP and mac are fixed

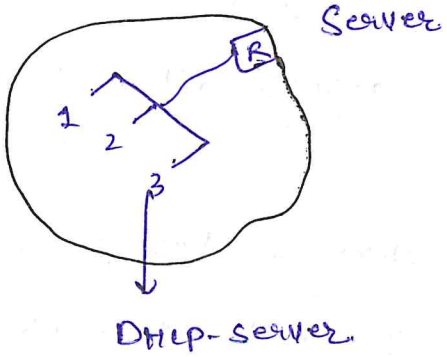
→ In the static table IP's are fixed so that we can not reuse them. Let suppose we have 10 systems and we are only using 3 system the rest of 7 systems IP's are not usable at that instant of time.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

DHCP (Dynamic host configuration Protocol)

→ Most widely used.
→ dynamic + static entries
→ relaying (Like in BOOTP)
→ lease time



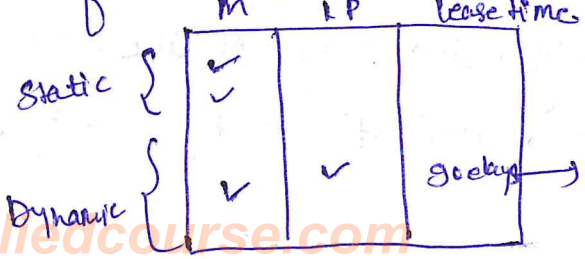
* In the DHCP there is also a concept of relaying like in BOOTP.

* Here we have dynamic as well as static entries in the DHCP server.

Static entries are for those systems who always connect with the internet like server [That are always on]

* Set of the IP addresses are available that are non-assigned. When a new computer connect DHCP server assigned one IP address amongs non-assigned IP address.

There is a concept of lease time when DHCP server assigned an address. It also assigned the lease time that is valid for that particular IP address.



Once the lease time is over. We need to again assign the IP address.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Private vs Public IP:

* We have only 2^{32} public IP addresses. To save the public IP addresses we use the concept of private IP- address.

* ISP has only Public Ip addresses which is limited to some number

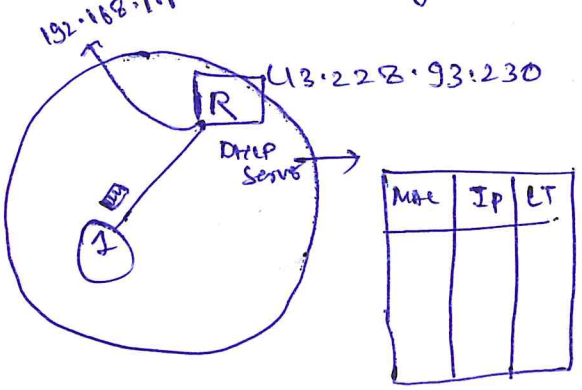
Private IP address:

10.0.0.0 to 10.255.255.255
172.16.0.0 to 172.31.255.255 [IANA]
192.168.0.0 to 192.168.255.255

These are the range of private IP address.

* We can effectively utilize the public IP addresses with the help of private IP addresses.

The public address will assign to router and rest of the system inside LAN will assign private addresses.



The host 1 is assigned with private IP address with the lease time by the router or DHCP server.

Gateappliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Host 1 sends the packet by

SA: 0104 private address Assigned by DHCP server

DA: 192.168.1.1 (Router internal address)

When router further sending the packet outside LAN.

SA: 43.228.93.230 (Public ~~Google~~ Address)

DA: Google Address.

* For getting IP address from DHCP server.

Sender sends. SA: 0.0.0.0 + MAC address → Broadcast packet.

* The router that converts your private address to public address while sending outside are called the NAT router. [Network Address Translation].

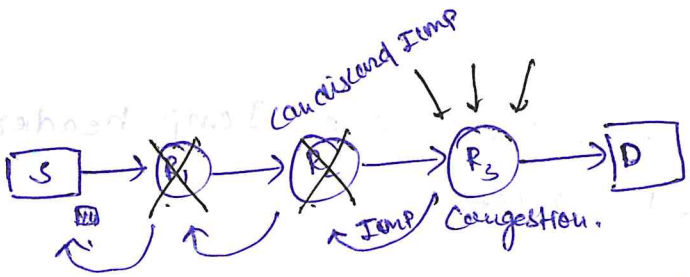
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

ICMP (Internet control message protocol.)

Internet Protocol (IP) → Unreliable → no ACK.
Datagram

Ex-1



packet crossed R_1, R_2. . At R_3 there is congestion

The Router R_3 discards the packet because of the congestion.

→ The Router 3 drops the packet so it will inform the source using Icmp. [sending Icmp is not mandatory]

IP + Icmp ⇒ Unreliable because Icmp packet can sometime be discarded.

→ TCP → reliable.

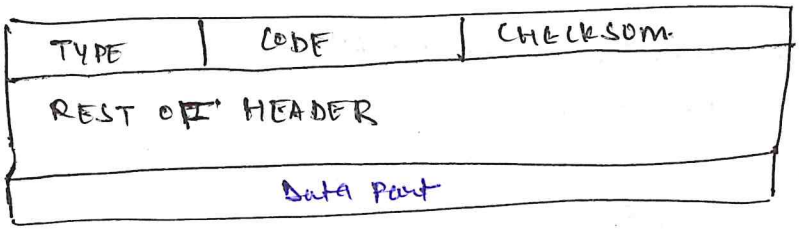
Icmp
- → can be discarded.
- → not mandatory.
- → ∞- loops.

* for the discarded Icmp packets we don't send Icmp again

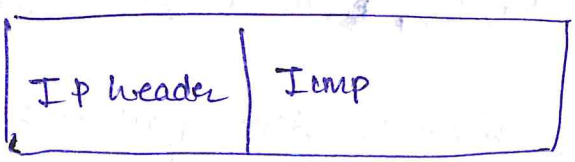
Gate-appliedcourse.com
gatecse@appliedcourse.com

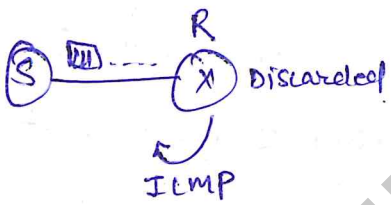
APPLIED COURSE
Ph: +91 844-844-0102

ICMP header format



* The ICMP packet sits inside the data part of IP packet



* 

* ICMP packet has header + Data part

* In the data part of ICMP packet we put the header of IP packet + 8 Bytes of data of IP packet

↓

This ICMP packet when reaches the sender. By looking at header and data part of ICMP packet. Sender get to know about which packet has been lost.

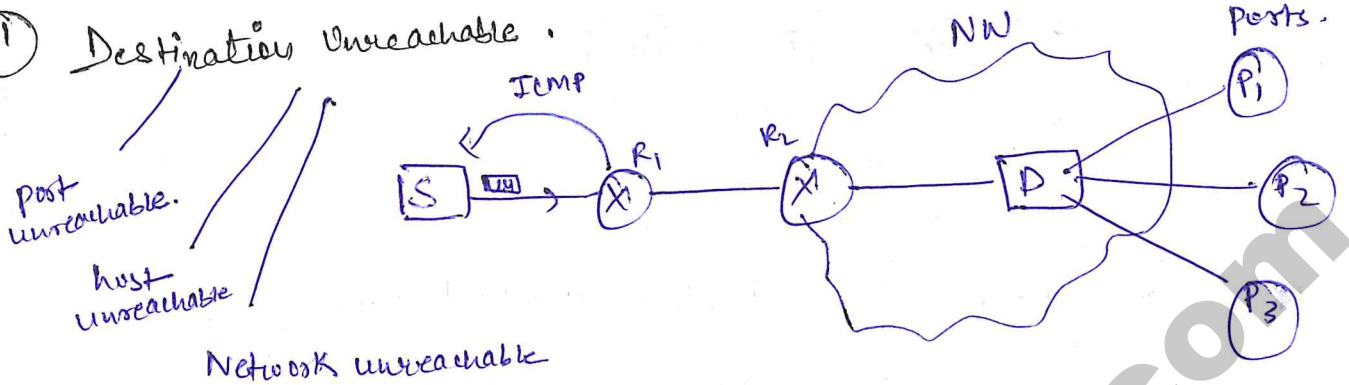
Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Types and code for Icmp: WIKI.

(1) Destination Unreachable.



(a) Post unreachable → The R_2 can not send the packet to portin D. So post unreachable.

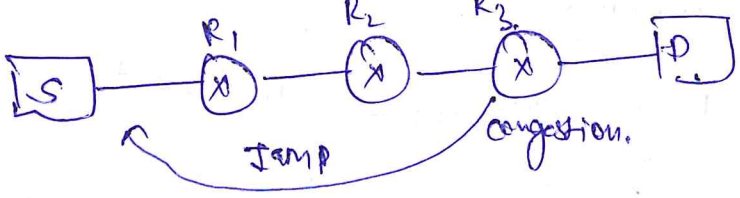
(b) Host unreachable → Host can be unreachable.

(c) Network → R_1 can not reach to NW.

* Ports helps us to send the packet in the specific program or process on the destination.

→ There are various types and codes are available in Icmp.

(2) Source quench: Type 4

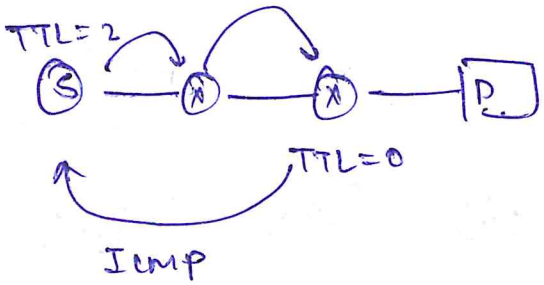


The Router 3 sends the ICMP packet to the source that stop sending the packets.

Gate.appliedcourse.com
gatecse@appliedcourse.com

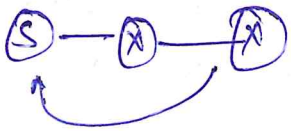
APPLIED COURSE
Ph: +91 844-844-0102

③ Time exceeded :



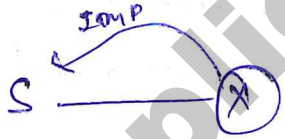
* TTL = 0 so send time exceeded message.

④ Parameter Problem : →



There is problem in Ip header. So router send an Icmp packet saying that header has some problem.

⑤ Router advertisement and solicitation :-



The router advertisement : I am the router that everyone should use.

Ping and Traceroute :

Ping google.com → echo request.

Try this on terminal ←

64 bytes from 172.217.167.174 icmp seq=0 ttl=53 time=19.942 ms
!
↓
echo Reply from ping command.

* Ping helps you to know everything is working perfectly.
Test / Debug network.

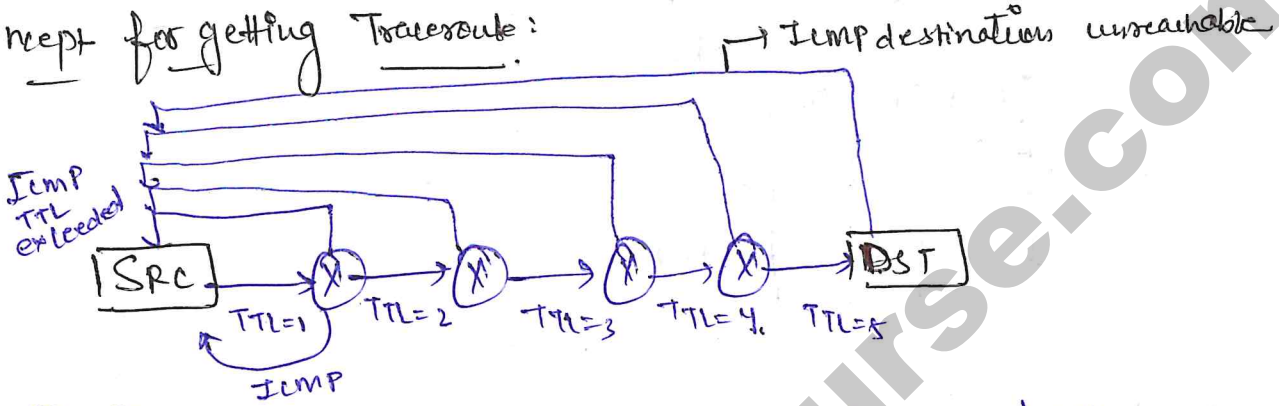
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Traceroute: Traceroute amazon.com

By using traceroute you will get to know the IP address of all the computer/router in the network in between amazon.com.

Concept for getting Traceroute:



(a) First we assign TTL=1 so packet goes from source to first router and we get the address of first router, because first router send the Icmp packet with message Icmp TTL exceeded

(b) Second we assign TTL=2 we get the address of 2nd router.

⋮

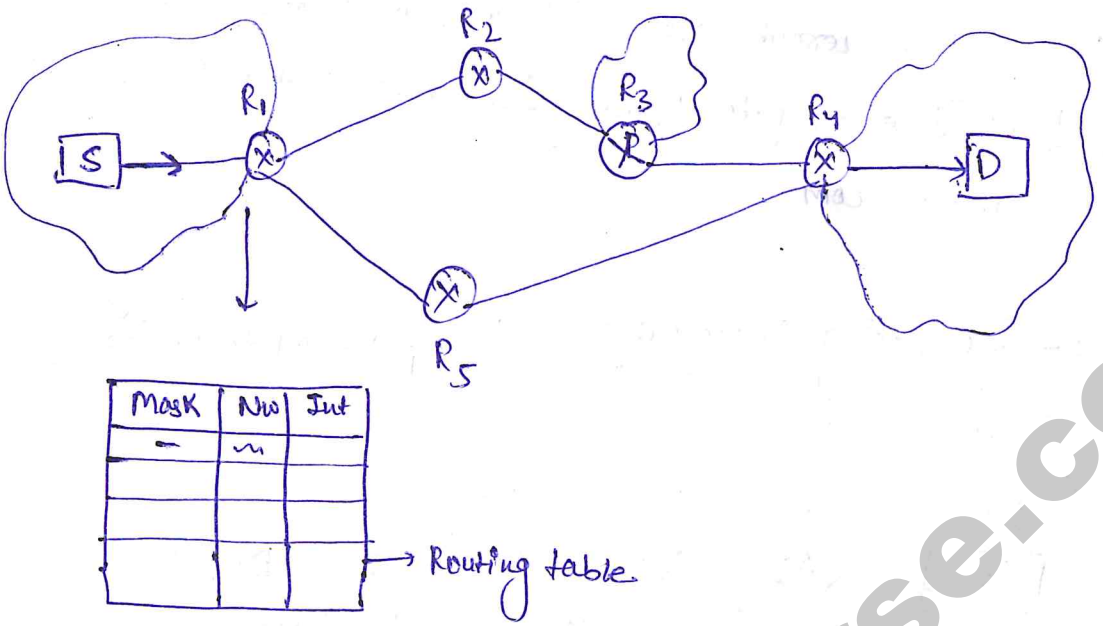
Like this we get the IP address of whole routers in the route.

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Routing:



* After seeing the destination address every router has to make this decision what is the next hop device.

* Routing is all about entries in routing table. How the packet will be guided by the routers to reach the destination.

* Routers interact with each other to fill the routing tables. Every router has the routing table.

- Routing Algo
  - Non-adaptive (Static)
    - flooding
    - Random-walk.
  - Adaptive (Dynamic)
    - Distance-vector
    - Link state algo.

Gate.appliedcourse.com
gatecse@appliedcourse.com

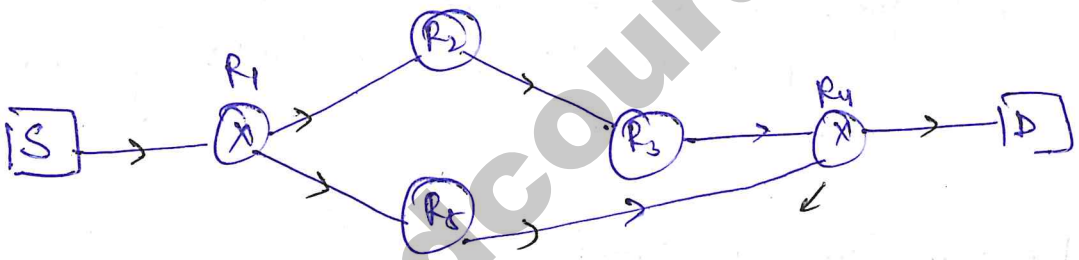
APPLIED COURSE
Ph: +91 844-844-0102

* Traffic changes over time and so congestion also changes. Topology also changes over time because of increment/decrement of router.

→ So there is change in graph therefore in Non-adaptive/static algorithms. we don't give worth to traffic and topology change.

* In Practical we use Adaptive/dynamic algorithms.

Flooding:



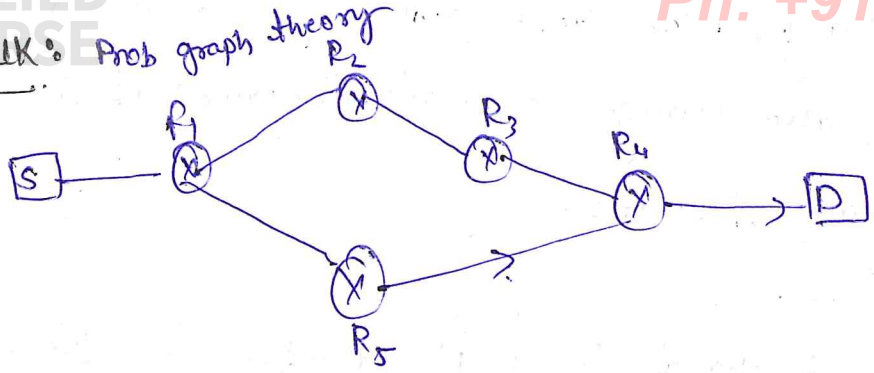
* In flooding whenever the router gets the packet it will flood to every other router in the path but except the point of origin.

* This will create congestion or looping.
* By flooding this is guarantee that if exists a single path from source to destination then the packet will reach.
* That makes flooding extremly reliable.
* Here we don't require any routing table.
* Atleast one packet will take the shortest path because we are taking every path.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Random walk: Prob graph theory



(1st) → Pick a router randomly [one technique] for sending the packet.

(2nd) technique: In this technique every router sends the packet to the least queued / busy router.

Distance-Vector-algo / routing

↓

Bellman-Ford-algo

↓

Subpaths of the shortest paths are shortest paths

If the shortest path u to v is given.
then the shortest path from u to w is also this.

Gate.appliedcourse.com

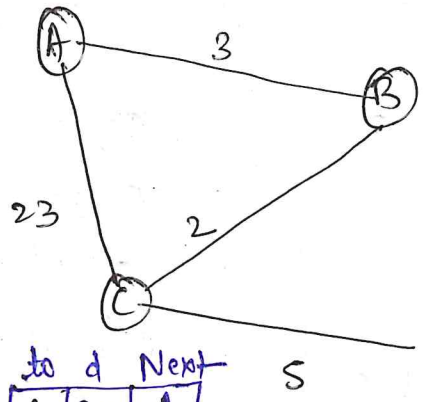
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Ex:-

A →

to	d	Next
A	0	A
B	3	B
C	23	C
D	∞	-



B →

to	d	Next
A	3	A
B	0	B
C	2	C
D	∞	-

C →

to	d	Next
A	23	A
B	2	B
C	0	C
D	5	D

D →

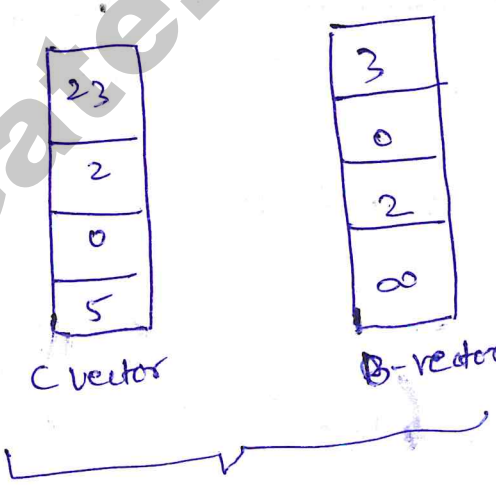
to	d	Next
A	∞	-
B	∞	-
C	5	C
D	0	D

→ Routing tables with 1 hop knowledge only

At time t = (1) → hop Every router A, B, C, D has the routing table and also knows its neighbour distances.

At time = (2) → hop we have to find the path length = 2

Now C, and B will send the distance vector to A



This information shared to A

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Now, A updates its distance vector using B and C.

A →

to	d	next hop
A	0	A
B	3	B
C	5 ~~23~~	C
D	28	C

A new table

23
2
0
5

AC: 23

3
0
2
∞

AB: 3

AtoD = AtoC = 23 BtoC = 5 = ~~8~~ 23+5 = 28.

AtoC = AtoB = 3 BtoC = 2 = 5

B also get distance vector from A and C.

B →

to	d	Next
A	3	A
B	0	B
C	2	C
D	∞	~~7~~

B new table

0
3
23
∞

A distance vector

BA: 3

23
2
0
5

C-distance vector

BC: 2

B to D = B to A + A to D

= 3 + ∞

= ∞

~~B~~ B to D = B to C + C to D

= 2 + 5 = 7

Gate.appliedcourse.com

gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Similarly C will get distance vector from A and B

C new table

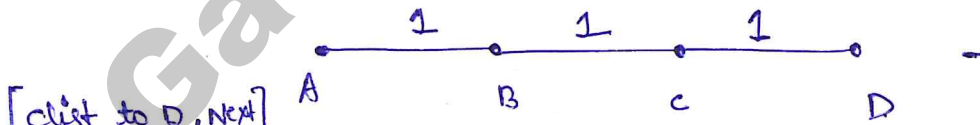
To	d	next
A	23	A
B	2	B
C	0	C
D	5	D

Similarly D will get distance vector from C

To	d	Next
A	28	C
B	7	C
C	5	C
D	0	D

* One iteration is completed.
* For distance vector we continue repeating this step because topology can change over period of time.

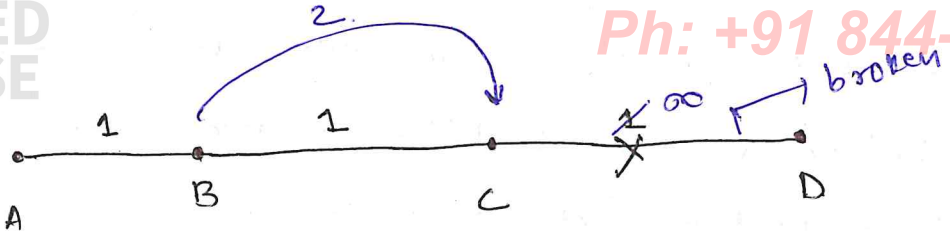
Count-to-∞ problem (topology changes)



→ Here we are writing a distance to D from all routers.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102



3, B 2, C 1, D

Exch-1 3, B 2, C 3, B ⇒ C will update 3 because distance of D using B is 2

Exch→2 3, B 4, C 3, B ⇒ B update distance using C

Exch→3 5, B 4, C 5, B ⇒ A updates distance using B

These distances keep increasing upto ∞.

So, packet Stuck in loop ⇒ A → B → C → B → C ∞ - loop.

Solution for count to ∞ problem is split Horizon:

t 3, B 2, C 1, D

t+1 3, B 2, C ∞, -

∞

∞ (as 'B' depends on 'C' to goto D)
So, B will not transfer distance vector to C

t+2 3, B ∞, - ∞, -

t+3 ∞, - ∞, - ∞, -

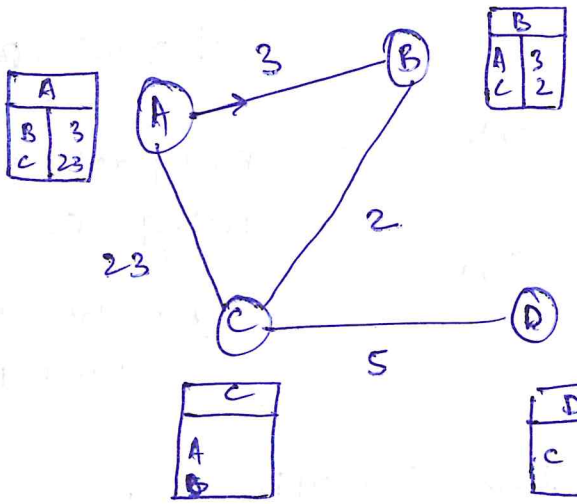
Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

→ for previous example of distance vector by using split horizon we only send the distance vector with ∞ to the next-hop node.

→ RIP uses distance vector routing

Link State Routing : (LSR)



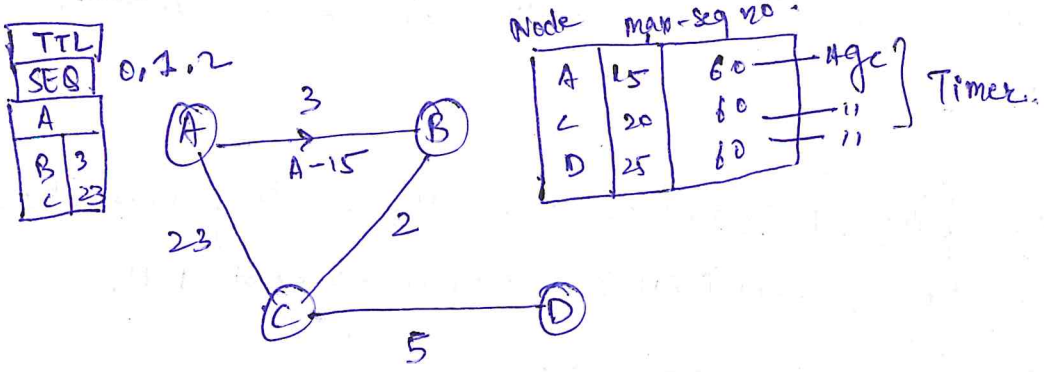
→ hello packets
→ flood link info
→ Dijkstra's algo
→ global knowledge

* Every node construct a packet containing information about the adjacent nodes. These are called linked state packets.
* Every link state packet is flooded to every other node.
* Now on A → C, B, D packets will reach.
* Once we have a whole information of all nodes we can construct a graph and run dijstra's algorithm for shortest path.
* Every vertex has the knowledge of every other vertex.
* OSPF (Open shortest path first) most widely used algorithm for link state.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

Sequence number :



* Sequence number is help us to keep track how network is keep changing and evolving over time.

* We add sequence number because if any node receives the packet with older sequence no. that packet will be discarded.

* Every node has the list of maximum sequence number. If we receive the packet less than the max^m sequence number than that packet will be discarded. It also reduce the congestion by discarding the packet.

* We discard duplicate packet to reduce flooding.

* We have a TTL field in the packet. So passing through every router we can decrease the TTL value. This will help us avoid Transient looping (Temporary looping) (non-persistent)

* If a node re-started ~~the~~ and sends a new fresh packet with sequence 0, the another node might think this is an old packet because of less sequence number.

Gate.appliedcourse.com
gatecse@appliedcourse.com

APPLIED COURSE
Ph: +91 844-844-0102

The solution for this problem is Age field where. after some time like 60 sec age field will expire. and maxm sequence number entry will be remove from node.

Que: Consider the following statements about the routing protocols, Routing Information protocol (RIP) and Open Shortest Path first (OSPF) in an IPv4 Network.

I. RIP uses distance vector routing

II. RIP packets are sent using UDP

III. OSPF packets are sent using TCP.

IV. OSPF operation is based on link-state routing.

Which of the following above are CORRECT?

(A) I and IV only
(B) I, II, III only
(C) I, II, IV only
(D) II, III, IV only.

Ans → I → correct (we already discussed in video)
II → RIP used UDP [remember that]
III → X
IV → correct (we already mentioned in video)

Que: Suppose that in an IP-over Ethernet network, a machine X wishes to find the MAC address of another machine Y in its subnet. Which one of the following techniques can be used for this?

(a) X sends an ARP request packet with broadcast IP address in local subnet.
(b) X sends an ARP request packet to the local gateways MAC address with then finds the MAC address of Y and sends to X
(c) X sends an ARP request packet with broadcast MAC address in its local subnet. [Already discussed in video]
(d) X sends an ARP request packet to the local gateway's IP address and then find the MAC address of Y and sends to X?

it sends with broadcast MAC address

gateclose@appliedcourse.com
Gate.appliedcourse.com